





Abschlussbericht

Einführungs- und Kommunikationsstrategien für IT Infrastrukturprojekte

Technische Universität München
Institut für Informatik,
Lehrstuhl für Wirtschaftsinformatik (I 17)
Prof. Dr. Helmut Krcmar
Boltzmannstr. 3, 85748 Garching b. München

Universität St. Gallen
Institut für Medien- und Kommunikationsmanagement
Prof. Dr. Miriam Meckel
Blumenbergplatz 9, 9000 St.Gallen

Autoren:

Manuela Obermeier, Cigdem Akkaya, Petra Wolf, Helmut Krcmar (TU München)

Miriam Meckel, Christian Pieter Hoffmann, Andrea von Kaenel (Universität St. Gallen)

Garching/St. Gallen, März 2012

INHALTSVERZEICHNIS

0. Vorwort ... 8

1. Einleitung ... 14

   1.1. Hintergrund und Motivation der Studie ... 14

   1.2. Zielsetzung der Studie ... 15

   1.3. Methodik ... 17

   1.4. Aufbau des Dokuments ... 17

2. Umfeldvoraussetzungen von eID-Infrastrukturprojekten ... 19

   2.1. Einleitung ... 19

   2.2. Faktoren, die die Akzeptanz von eID-Projekten beeinflussen ... 19

      2.2.1. Innovationsbezogene Einflussfaktoren ... 22

         2.2.1.1. Akzeptanzfaktoren nach Rogers ... 23

         2.2.1.2. Beispiele innovationsbezogener Faktoren ... 28

      2.2.2. Personenbezogene Faktoren ... 34

         2.2.2.1. Personenbezogenen Faktoren nach Rogers ... 34

         2.2.2.2. Weitere bedeutende personenbezogene Faktoren ... 34

         2.2.2.3. Beispiele personenbezogener Faktoren ... 39

      2.2.3. Vertrauensstufen bei E-Government-Dienstleistungen ... 44

      2.2.4. Übersicht: Nutzer- und Innovations-Charakteristika ... 50

3. eID-Projekte in Europa ... 55

   3.1. Internationaler Vergleich von eID-Infrastrukturen ... 56

      3.1.1. Belgien ... 58

      3.1.2. Großbritannien ... 59

      3.1.3. Finnland ... 61

      3.1.4. Österreich ... 62

      3.1.5. Spanien ... 64

      3.1.6. Zusammenfassung ... 65

      3.1.7. Folgerungen hinsichtlich des Marktpotenzials ... 67

4. Marktchancen für eID-Infrastrukturen in Deutschland ... 70

4.1. Vorgehen zur Ermittlung von Marktchancen ... 70

4.2. Marktanalyse für die Einführung des nPA in Deutschland ... 70

4.2.1. Marktabgrenzung ... 72

4.2.2. Akteure ... 73

4.2.2.1. Anbieter ... 73

4.2.2.2. Nutzer ... 74

4.2.2.3. Partner ... 76

4.2.2.4. Forschungsakteure ... 77

4.2.2.5. Intermediäre ... 77

4.2.2.6. Legislative ... 77

4.2.2.7. Wettbewerber ... 78

4.2.3. Interaktion zwischen den Akteuren ... 79

4.3. Marktcharakteristika der eID-Infrastrukturen in Deutschland ... 82

4.3.1. Eintrittsbarrieren ... 82

4.3.1.1. Politik des Staates ... 83

4.3.1.2. Kundenumstellung ... 83

4.3.1.3. Kapitalerfordernis ... 83

4.3.1.4. Zugang zu Vertriebskanälen ... 84

4.3.2. Timing der Markteinführung ... 85

4.3.3. Strategieoptionen für die Markteinführung ... 86

4.4. eID-basierte Geschäftsmodelle ... 91

4.4.1. E-Government-Geschäftsmodell nach Peinel ... 92

4.4.2. Grafische Darstellung der BMeG Modellierungsmethode ... 94

4.4.2.1. BMeG am Beispiel ‚Kfz-Zulassung' ... 94

4.4.2.2. BMeG am Beispiel ‚ELSTER' ... 95

4.4.2.3. BMeG am Beispiel ‚Emissionshandel' ... 96

4.4.2.4. BMeG am Beispiel ‚Gewerbeanmeldung' ... 97

4.4.2.5. BMeG am Beispiel ‚Gesamtauskunft' ... 98

4.4.3. Kritische Erfolgsfaktoren für den Markteintritt ... 99

4.5. eID-Anwendungsszenarien ... 100

4.5.1. Erhebung der Daten und Analyse der ausgewählten Szenarien (Methodik)........... 101

4.5.1.1. Kfz-Zulassung 102

4.5.1.2. ELSTER 109

4.5.1.3. Emissionshandel 115

4.5.1.4. Gewerbeanmeldung 123

4.5.1.5. Gesamtauskunft 132

5. Kommunikationsstrategien für eID-Projekte in Deutschland 141

5.1. Vorgehen bei der Ermittlung der Kommunikationsstrategien 143

5.2. Kommunikationsstrategien der Anwendungsszenarien 144

5.2.1. Kfz-Zulassung 144

5.2.2. ELSTER 145

5.2.3. Gewerbeanmeldung 148

5.2.4. Emissionshandel 149

5.2.5. Gesamtauskunft 151

5.2.6. Zusammenfassung 152

5.3. Generalisierung der Kommunikationsstrategien 154

5.3.1. Differenzierung der Kommunikationsstrategien 155

5.3.1.1. Zentrale Strategie 155

5.3.1.2. Dezentrale Strategie 155

5.3.1.3. Drittpartei-Strategie 156

5.3.2. Vergleich der Kommunikationsstrategien 156

6. Zusammenfassung und Handlungsempfehlungen 161

6.1. Markteinführungsstrategie für eID-Infrastrukturen 161

6.2. Kommunikationsstrategie für eID-Infrastrukturen 162

TABELLENVERZEICHNIS

Tabelle 1: Verschiedene Authentifizierungsmethoden (Clarke 1994) 30
Tabelle 2: Lösungsauswahlfaktoren (Information & Communications Technology branch) 33
Tabelle 3: Potentielle Auswirkungen von Authentifizierungsfehlern für E-Governmen-Dienste in den USA (Executive Office of the President 2003, 6ff.).. 47
Tabelle 4: Benötigte Vertrauensstufen für E-Government-Dienste in den USA (Executive Office of the President 2003) 48
Tabelle 5: Benötigte Vertrauensstufen für E-Government-Dienstleistungen in Großbritannien (UK Cabinet Office 2002, 16ff.) 49
Tabelle 6: Zusammenfassung des Ländervergleichs (Quelle: Eigene Darstellung) 67
Tabelle 7: Segmentierung der Bürger (Quelle: In Anlehnung an (Turner et al. 2005, 443)................. 74
Tabelle 8: Modellierungsentitäten einer Wertschöpfungskette des BMeG Modells (Peinel 2008, 66ff).. 93

ABBILDUNGSVERZEICHNIS

Abbildung 1: Komponenten des Projektes ... 16
Abbildung 2: Phasen und Komponenten Mapping und ihre verantwortlichen Projektpartner ... 16
Abbildung 3: Das Zusammenwirken von Innovations- und Nutzercharakteristika (Quelle: Eigene Darstellung) ... 22
Abbildung 4: Abwägung von Vertrauen und Sorgen (eigene Darstellung) ... 37
Abbildung 5: Wichtigkeit verschiedener Aspekte bei der elektronischen Abwicklung von Behördengängen im Internet (o. V. 2010a, 13) ... 41
Abbildung 6: Nutzungsbarrieren für E-Government-Angebote (o. V. 2010a, 14) ... 41
Abbildung 7: Bedenken speziell beim Datenschutz (o. V. 2010a, 14) ... 42
Abbildung 8: Persönlicher Mehrwert durch E-Government-Angebote in Deutschland 2010 (o. V. 2010a, 10) ... 50
Abbildung 9: Geplante Nutzung von Funktionen des neuen Personalausweises in Deutschland 2010 (o. V. 2010a, 15) ... 51
Abbildung 10: EU-weiter Status der Einführung von Personalausweisen mit eID-Funktion (Quelle: Eigene Darstellung in Anlehnung an (Assar 2011, 85) ... 56
Abbildung 11: Markt für den neuen Personalausweis in Deutschland ... 71
Abbildung 12: Interaktion zwischen Bürger, Staat und Intermediären (Quelle: Eigene Darstellung) .. 79
Abbildung 13: Gegenseitiges Authentifizieren (Quelle: Eigene Darstellung) ... 80
Abbildung 14: Interaktion zwischen Unternehmen, Angestellte und Staat (Quelle: Eigene Darstellung) ... 81
Abbildung 15: Interaktion zwischen Dienstanbieter, Verwaltung und Zertifikatvergabestelle (Quelle: Eigene Darstellung in Anlehnung an(Reisen 2009, 6) ... 82
Abbildung 16: E-Government Lösung (In Anlehnung an Scheer/Kruppke/Heib 2003, 36) ... 86
Abbildung 17: BMeG am Beispiel ‚Kfz-Zulassung‘ (Quelle: Eigene Darstellung) ... 94
Abbildung 18: BMeG am Beispiel ‚ELSTER‘ (Quelle: Eigene Darstellung) ... 95
Abbildung 19: BMeG am Beispiel ‚Emissionshandel‘ (Quelle: Eigene Darstellung) ... 96
Abbildung 20: BMeG am Beispiel ‚Gewerbeanmeldung‘ (Quelle: Eigene Darstellung) ... 97
Abbildung 21: BMeG am Beispiel ‚Gesamtauskunft‘ (Quelle: Eigene Darstellung) ... 98
Abbildung 22: Komponenten des neuen Personalausweises (Bundesministerium für Wirtschaft und Technologie 2008, 8) ... 99
Abbildung 23: Ausgewählte Szenarien (Quelle: Eigene Darstellung) ... 101
Abbildung 24: EPK der Kfz-Zulassung ohne nPA (Quelle: Eigene Darstellung) ... 105
Abbildung 25: Kfz-Zulassung mittels nPA (Quelle: In Anlehnung an (Löhe/Tschichholz 2010) ... 106
Abbildung 26: EPK der Kfz-Zulassung nach nPA-Einführung (Quelle: Eigene Darstellung) ... 108

Abbildung 27: EPK vor nPA-Einführung (Quelle: Eigene Darstellung) 112
Abbildung 28: EPK ELSTER nach nPA-Einführung (Quelle: Eigene Darstellung) 114
Abbildung 29: EPK Emissionshandel ohne nPA (Quelle: Eigene Darstellung) 118
Abbildung 30: EPK Emissionshandel nach nPA-Einführung 122
Abbildung 31: EPK vor nPA-Einführung (Quelle: Eigene Darstellung) 126
Abbildung 32: EPK Gewerbeanmeldung nach nPA-Einführung (Quelle: Eigene Darstellung) 130
Abbildung 33: Gewerbeanmeldung ohne nPA (Quelle: In Anlehnung an (DIHK 2009, 12) 131
Abbildung 34: EPK Gesamtauskunft vor nPA-Einführung (Quelle: Eigene Darstellung) 134
Abbildung 35: EPK Gesamtauskunft nach nPA-Einführung (Quelle: Eigene Darstellung) 137
Abbildung 36: Anspruchsgruppen eines kommerziellen Angebots (Rüegg-Stürm 2003) 141
Abbildung 37: Unterschiedliche Schwerpunkte von Kommunikationsstrategien 143
Abbildung 38: Website des ELSTER-Angebots 147
Abbildung 39: Differenzierung von drei Kommunikationsstrategien 155
Abbildung 40: Vergleich der Kommunikationsstrategien 158

0. Vorwort

„Denk` ich an den nPA in der Nacht[1]…..,

Das Projekt Einführungs- und Kommunikationsstrategien für IT-Infrastrukturprojekte startete von der Prämisse aus, dass es ein erfolgreiches eID-Einführungsprojekt wissenschaftlich zu begleiten gilt, um von den dort ergriffenen Maßnahmen zu Einführung und Kommunikation und deren Wirkung Good Practices und Handlungsempfehlungen abzuleiten. Im Gegensatz zu dieser Prämisse konnten wir ein eID-Einführungsprojekt nahezu ohne begleitende Maßnahmen zur Einführung und Kommunikation beobachten, abgesehen von einer Reihe von Pilottests, die von Öffentlichkeit nicht wahrgenommen wurden. In der Folge musste der Projektansatz dahingehend geändert werden, dass zunächst literaturbasiert Erkenntnisse zur Einführung von IT-Innovationen und Faktoren im Hinblick auf Nutzerpräferenzen und speziell den Aspekt des Vertrauens gegenüber eID Infrastrukturen gesammelt wurden. Im empirischen Teil der Studie wurde einerseits die erwähnte Umfrage begleitet und zudem Interviews mit Ansprechpartnern der Pilotpartner geführt. Diese waren allerdings von der Erkenntnis begleitet, dass das aktuell nutzbare Potenzial der nPA-Infrastruktur, insbesondere aus Bürgerperspektive, sehr begrenzt ist.

Im Folgenden die im Rahmen der Studie gewonnenen Erkenntnisse anhand einiger Thesen zusammengefasst:

1. Netzeffekte sind ausschlaggebend für den Einführungserfolg

2. „If we build it, they will come" – Implementierung x Einführung x Nutzung (Krcmar 2009, 12) in Anlehnung an (Markus/Keil 1994)

3. Mobilisierung des nPA unerlässlich

1. Netzeffekte sind ausschlaggebend für den Einführungserfolg

Das Projekt Einführungs- und Kommunikationsstrategien für IT Infrastrukturprojekte (eKIT) wurde von der Technischen Universität München in Zusammenarbeit mit der Universität St. Gallen unter Förderung von ISPRAT durchgeführt. Zielsetzung der Studie laut Projektantrag war es Einführungs- und Kommunikationskonzepte für IT-Infrastrukturprojekte am Beispiel des nPA bzw. der AusweisApp zu differenzieren und zu bewerten. Im Rahmen des Projektes eKIT sollten die Anforderungen der relevanten Akteure analysiert, die Kommunikation verschiedener Anwendungsfälle unter-

[1] dann bin ich um den Schlaf gebracht" (in Anlehnung an H. Heine)

sucht, und konkrete Gestaltungsempfehlungen für weitere Infrastrukturprojekte am Beispiel des nPA bzw. der Ausweis App entwickelt werden. Aus den gewonnenen Erkenntnissen sollten Gestaltungsempfehlungen für künftige IT Infrastrukturprojekte am Beispiel des nPA/der AusweisApp abgeleitet werden.

Es sollten vor allem Aspekte wie Einfachheit, Vertrauen und Marktchancen beleuchtet werden. Da einige der pilotierten Anwendungsfälle der öffentlichen Verwaltung immer noch der Schriftform bedürfen und dieses Problem noch nicht gelöst ist, für Anwendungen der Privatwirtschaft, wie Online-Banking und eBay allerdings bereits Lösungen (z. B. mobile Banking, PayPal) existieren, haben wir uns in diesem Projekt auf Anwendungsfälle des öffentlichen Sektors konzentriert.

An dieser Stelle stellt sich die Frage, warum es bislang nur so wenige Anwendungsfälle gibt, in denen der nPA mit all seinen Vorzügen eingesetzt werden kann. Das Problem ist, dass in Deutschland für die Sicherstellung der Rechtsgültigkeit von Verträgen und Behördenkontakten in den meisten Fällen immer noch die Schriftform erforderlich ist. Durch dieses Erfordernis werden Neuerungen wie bspw. die Nutzung des nPA gehemmt. Hier ist vonseiten des Staates mehr Mut nötig: Durch die Einführung eines E-Government-Gesetzes müssen verschiedenste Gesetze geprüft und ggf. neu geordnet/überarbeitet werden. In einem E-Government-Gesetz muss verankert werden, dass auch mittels elektronischem/digitalem Identitätsnachweises die Schriftform erfüllt wird.

Der nPA sollte den Bürgern helfen sowohl Zeit als auch Geld einzusparen und gleichzeitig das Internet für Kontakte zur Verwaltung zu nutzen (Bundesministerium des Inneren 2010b, 1). Durch die nötige Schriftform für viele Behördenkontakte wurde bisher allerdings weder Zeit noch Geld eingespart. Im Gegenteil entsteht durch die Aufteilung von Behördenkontakten in elektronische und persönliche/schriftliche Bearbeitungsbereiche zusätzlicher Aufwand und Arbeit.

Gleichzeitig sind die bisher wenigen Nutzerszenarien eher anbieterorientiert gestaltet und nicht auf die Bedürfnisse der Bürger ausgerichtet. Um das Interesse der Nutzer zu wecken, muss allerdings vor allem ihnen ein entstehender Mehrwert durch die Benutzung des nPA aufgezeigt werden. Dafür ist es wichtig die Anwendungsfälle und Szenarien endnutzerorientiert zu gestalten (Grote et al. 2010, 4).

Wären die nötigen Voraussetzungen von rechtlicher Seite gegeben und würden vonseiten des Staates Anreize für die Nutzer geschaffen, würde auch die Attraktivität des gesamten nPA-Netzwerks für seine Nutzer steigen. Denn Nutzer sorgen für Nachfrage nach Anwendungen, diese bringen mehr Potenzial wodurch wiederum mehr Nutzer gewonnen werden und wertvolle Netzwerkeffekte entstehen. Jeder zusätzliche Nutzer steigert den Wert des Netzwerks und somit auch die Anzahl der entwickelten systemspezifischen Produkte und der Anwendungsfälle. Positives Feedback der Nutzer trägt zu weiterem positiven Feedback anderer Nutzer bei und zur Entwicklung weiterer Netzwerkprodukte und Anwendungen (Zerdick et al. 2001, 156ff). Es ist daher wichtig, Nutzungsanreize zu schaffen, um ein

Netzwerk um den nPA aufzubauen, damit die Attraktivität des nPA für Bürger und andere Nutzer sowie die Anzahl der Anwendungsfälle steigen (Krcmar 2009, 15).

Damit potenzielle Nutzer dem neuen Personalausweis eine Chance geben und oben genannte Netzeffekte entstehen können, müssen zwei Prämissen erfüllt sein. 1. Die Nutzer des nPA müssen von einer gewissen Kompetenz des Staates in Bezug auf Sicherheit im Netz überzeugt sein und 2. auf die Motivation des Staates zum Datenschutz vertrauen. Jedoch ist die dafür nötige Transparenz in den wenigsten Fällen gegeben, da viele Bürger und Nutzer die Technologie, die hinter dem nPA steht nicht nachvollziehen können. Mit der fehlenden Transparenz fehlt auch das Vertrauen und die nötige bürgerliche Unterstützung bei der Einführung und Nutzung des nPA (Grote et al. 2010, 3).

2. If we build it, they will come – Wert = Entwicklung x Deployment x Nutzen (Krcmar 2009, 12) in Anlehnung an (Markus/Keil 1994)

Der Wert einer neuen Technologie ist gleich Entwicklung mal Deployment mal Nutzen bzw. Nutzung. Verbindet man die drei Aspekte, Entwicklung von technischen Innovationen, Deployment von technischen Innovationen und Nutzung von technischen Innovationen multiplikativ miteinander, so wird deutlich, dass, wenn bspw. die Nutzung gleich null wäre, auch die Entwicklung und das Deployment von Innovationen keinen Sinn hat (Krcmar 2009, 12). Das bedeutet, dass so schnell wie möglich ein Angebot für Bürgerservices aufgebaut werden muss, damit der Nutzen des nPA endlich zur Geltung kommt.

Die Entwicklung des nPA wurde erfolgreich abgeschlossen/gelöst, sodass an dieser Stelle keine Probleme entstanden.

Das Deployment betrifft in diesem Fall vor allem die Verbreitung der Lesegeräte. Der nPA soll eingesetzt werden, um die Authentifizierung eines Benutzers gegenüber einem Dienstleister sicherer und einfacher zu gestalten. Jedoch wurden die dafür nötigen Lesegeräte erst verspätet (nach dem 01.11.2010) zur Verfügung gestellt. Zum Misserfolg der Einführung des nPA trug außerdem die Tatsache bei, dass anfangs nur 1.000 Lesegeräte bereitgestellt werden konnten.

Sobald der Bürger einen nPA ergattert hat, steht er vor einem weiteren Problem: Es gibt insgesamt drei verschiedene Varianten des Lesers mit unterschiedlichen Funktionen und Sicherheitslevels. Setzt man einen sogenannten Basisleser ein und gibt deswegen die PIN über die Tastatur eines Computers ein, besteht ein höheres Restrisiko, dass Eingaben bei einem Befall durch Malware mitgelesen werden. Im schlimmsten Fall kann der Angreifer die Identität des betroffenen Benutzers bei jedem Dienstleister willkürlich verwenden, was ein enormes Sicherheitsproblem darstellt. Die anderen zwei Lesegeräte, Standard- und Komfortleser, ermöglichen hingegen eine Eingabe über das Pinpad des Geräts und besitzen dadurch ein geringeres Restrisiko (Dietrich et al. 2010, 4f). Bürger stehen somit vor der Qual

der Wahl und müssen sich zuerst über Preis, Funktion und Sicherheit der drei Geräte informieren, anschließend Vor- und Nachteile abwägen und eine Entscheidung für ein Gerät treffen. Jeder potentielle Nutzer sollte über die eID-Funktion, die vorhandenen Lesegeräte und die unterschiedlichen Sicherheitslevel informiert werden, um von den Funktionen des nPA einfach und sicher Gebrauch machen zu können. Ein wesentliches Manko bei der Einführung des nPA war, dass die Nutzer über die genannten Unterschiede der Lesegeräte nicht offensiv informiert wurden. Erst wenn ein Bürger sich selbst mit dem nPA auseinandergesetzt hat, wurde ihm bewusst, dass es Unterschiede bei der Hardware gibt. Nicht nur zu Informationszwecken, sondern auch um den nPA populär zu machen und den Benutzern näher zu bringen, ist es dafür unerlässlich Werbeaktionen und Aufklärungskampagnen zu starten. Es wurde darüber hinaus keine Werbung geschaltet, in der man darüber informiert wird, wo man die AusweisApp downloaden/beziehen kann.

Nutzen kommt von Nutzung und demensprechend war aufgrund der wenigen vorhandenen Informationen wie bspw. über den Bezug der AusweisApp die Nutzung für Bürger nicht ergonomisch genug, wodurch das Verhalten der Bürger hinsichtlich der Nutzung des nPA restriktiv war. Da die Nutzung für Bürger nicht ergonomisch ist, konnte dadurch für sie auch kein Nutzen entstehen.

Der Markt für eine AusweisApp ist nicht vorhanden, obwohl wir eigentlich erwartet hatten, dass sich im Laufe der Zeit ein Markt entwickeln würde – dem war aber nicht so. Am deutlichsten wird das Dilemma, wenn man andere Themenbereiche betrachtet: was wäre der iPod ohne mp3 oder ein Smartphone ohne Apps? - Nur mäßige Technik ohne Nutzen!

Die Formel für den nPA heißt also: Wert = 1 (Entwicklung) x 0 (Deployment) x 0 (Nutzen) = 0, das heißt ein Wert bzw. Einführungserfolg des nPA ist nicht vorhanden, da sowohl Deployment/Ausrollen des nPA und dessen Equipment als auch ein Nutzen nicht vorhanden sind.

Am Anfang des Projektes sind wir davon ausgegangen, dass man etwas lernen kann, wenn man die Einführung des nPA begleiten darf. Doch leider konnten verschiedenste Aspekte des Projektes aufgrund der mangelnden Anwendungen und Nutzung nicht untersucht werden. Auf so etwas waren wir nicht vorbereitet: Am Ende der Untersuchung kommen wir zu dem Schluss, dass die Einführung des nPA ein Misserfolg war. Eine solches Projekt setzt eine Einführungs- und Kommunikationsstrategie voraus und nicht eine NICHT-Einführungs- und NICHT-Kommunikationsstrategie. Es gibt derzeit über die bereits existierende Forschung von bspw. Mertens, der sich mit existierenden Schwierigkeiten und Problem bei IT-Projekten in der öffentlichen Verwaltung beschäftigt, hinaus, keine neuen Erkenntnisse. Basierend auf einer Untersuchung von sieben gescheiterten IT-Projekten der öffentlichen Verwaltung identifizierte Mertens (2009, 46ff) unterschätze Komplexität, falsche Relation zwischen der Vorbereitungszeit und der Umsetzungszeit, eine zu große Anzahl an Change Requests und beispielsweise Ausschreibungsprobleme als Hauptschwierigkeiten bei der Projektumsetzung. Er empfiehlt einen dreiphasigen Projektablauf, bestehend aus Vorbereitung, Funktionalausschreibung und der

anschließenden Realisierung, sowie die Durchführung von Methoden, die seit langer Zeit im Bereich des Software Engineering (z.B. Pflichtenheft, Stakeholderanalyse) und Projektmanagement (z.B. Netzplantechnik) etabliert sind. Außerdem schlägt er vor, eine sogenannte Fachspezialistenlaufbahn im öffentlichen Dienst einzuführen um die Kluft zwischen Beamten, welche auf IT spezialisiert sind und hochspezialisierten Beratern zu überbrücken. Der Bedarf an Fachkräften ist auch in IT-Projekten hoch und sollte gedeckt werden, damit Projekte erfolgreich abgeschlossen werden können.

Die missglückte Einführung des nPA bedeutet allerdings nicht seinen sofortigen Todesstoß, sondern zeigt, dass es an dieser Stelle noch genug Verbesserungspotenzial gibt (z B. Ideenwettbewerbe für App-Entwicklung). Des Weiteren verfügt der nPA derzeit über einige verpflichtende, aber auch über optionale Funktionen, wie bspw. die eID-Funktion. Das Problem bei Wahlmöglichkeiten ist, dass man sich dafür oder dagegen entscheiden kann. Entscheidet man sich also gegen die eID-Funktion, so können die eigentlichen Vorteile, die der nPA mit sich bringt, nicht genutzt werden. Dies hat zwar vor allem Nachteile für den jeweiligen Bürger selbst, aber auch für die Gemeinschaft, da dadurch mögliche Netzeffekte nicht entstehen können. Eine Lösungsmöglichkeit dieser Tatsache entgegenzuwirken, wäre die Zwangsfreischaltung der eID-Funktion, ohne Mehrkosten, sodass die Hemmschwelle für den Ein oder Anderen niedriger ist etwas Neues auszuprobieren. Denn mit jedem zusätzlichen Nutzer, steigt der Wert des Netzwerks (Krcmar 2009, 13).

Eine Lösung, um die mangelnde Anzahl von Apps in den Griff zu bekommen wäre, den Kontext zu ändern. Da, wie bereits erwähnt, in Deutschland immer noch die Schriftform erforderlich ist, ist der Einsatz des nPA noch überflüssig. Dem könnte entgegengewirkt werden, indem im E-Government-Gesetz verankert wird, dass auch mittels nPA die nötigen Voraussetzungen für einfache und sichere Kontakte zwischen Verwaltung und Bürger bzw. Unternehmen gegeben sind.

3. Mobilisierung des nPA ist unerlässlich

Durch die zunehmende Mobilisierung, ist eine Zukunftsvision für die Nutzung des nPA sicherlich dessen Mobilisierung. Das heißt, dass es möglich werden muss, den nPA mittels Smartphone auslesen zu können. Für ein Land das Elektroautos baut, muss es möglich sein dieser Forderung nachzukommen. Es muss also möglich sein, dass der nPA auch für mobile Anwendungen eingesetzt werden kann.

Eine Möglichkeit, wie man den nPA mobil nutzen könnte ist, ihn mittels NFC Technologie auszulesen. Fast jeder Jugendlich besitzt heutzutage ein Smartphone und auch andere Generationen können ohne nicht mehr leben. Die Menschen drängen nach Mobilität, nach Erreichbarkeit und nach Komfort. Sie wollen auf Dienste und auf Kontakte jeder Zeit und an jedem Ort zugreifen können. Dies bezieht sich auch auf Verwaltungskontakte und damit auch auf die Funktionen des nPA. Die momentane technische Umsetzung der nPA-Funktion steht jedoch genau im Widerspruch zu diesem Trend, da sie nur

stationär von zu Hause aus genutzt werden kann. Deswegen sollte es möglich sein, den nPA auch mittels NFC Handy/Smartphone auszulesen. Nicht zuletzt können dadurch viele neue Anwendungsfälle geschaffen werden, in denen der nPA eingesetzt werden kann. Erste Entwicklungen sind an verschiedenen Stellen bereits im Gang und müssen mit Nachdruck und entsprechenden Kommunikationsoffensiven begleitet werden.

Zusammenfassend kann festgehalten werden, dass das Gesamtkonzept des nPA zu wenig durchdacht war. Da den Bürgern von Anfang an nicht klar vermittelt wurde, wozu ein neuer Personalausweis benötigt wird und welchen Nutzen dieser für sie bietet, akzeptieren viele Bürger den neuen Personalausweis und dessen Funktionalität nicht. An dieser Stelle wäre es Aufgabe der Behörden/des Staates ein zielgruppenorientiertes Marketing zu etablieren, denn wenn Bürger die Vorteile des nPA kennen, erhöht sich auch dessen Akzeptanz. Erst die Kombination aus Infrastruktur und Angeboten bringt einen Nutzen für alle Beteiligten. Letzten Endes sind Nutzen, Sicherheit und Netzeffekte wesentliche Bestimmungsfaktoren für den weiteren Erfolg des nPA. Zum einen müssen für Bürger genügend Anreize geschaffen werden, sich den nPA mit allen Funktionen freischalten zu lassen. Zum anderen müssen aber auch die Prozesse und Rahmenbedingungen der Verwaltung entsprechend angepasst bzw. verbessert werden um künftig die Vorteile des nPA ausschöpfen zu können (Krcmar 2009, 28).

Garching, im März 2012 Helmut Krcmar

1. Einleitung

1.1. Hintergrund und Motivation der Studie

Laut deutschem Gesetz sind alle Bürger über 16 Jahren dazu verpflichtet, einen Personalausweis zu besitzen und diesen auf Anfrage vorzuzeigen (Bundesministerium der Justiz 2010a). Im November 2010 wurde der neue Personalausweis (nPA) eingeführt. Das Hauptziel der Einführung ist die Erweiterung des konventionellen Personalausweises um elektronische Funktionen und die damit einhergehende Anpassung an die Herausforderungen und Möglichkeiten des 21. Jahrhunderts. Neben der Identifikationsfunktion ist die Nutzung als europäisches Reisedokument ein weiterer Vorteil des nPA. Gleichzeitig kann er für Onlineanwendungen im privaten Sektor genutzt werden.

Folgende Komponenten sind für die elektronische Nutzung des nPA notwendig (Bundesamt für Sicherheit in der Informationstechnik 2011b):

1. AusweisApp: Software für die Authentifizierung zwischen E-Business-Unternehmen bzw. Behörden und dem Ausweisbesitzer. Die AusweisApp ist eine Client-Middleware-Software, die auf dem „eCard API Framework" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) basiert (Bundesamt für Sicherheit in der Informationstechnik 2011a).
2. Internetfähiger Computer.
3. Internetzugang.
4. Kartenlesegerät (verschiedene Typen sind erhältlich).

Traditionell ist die Akzeptanz der Nutzer eine Herausforderung im Rahmen von E-Government-Projekten, da Bürger regelmässig den Nutzen von E-Government nicht erkennen (o. V. 2010a, 10ff). Aus diesem Grund befasst sich das Projekt eKIT (Einführungs- und Kommunikationsstrategien für IT Infrastrukturprojekte) mit Fragestellungen wie der ‚Einfachheit' des Angebots, dem ‚Vertrauen' der Nutzer sowie Marktmöglichkeiten, nicht nur für die AusweisApp im Speziellen, sondern für den digitalen Ausweis als innovatives E-Government-Angebot in Deutschland.

Bevor auf Aspekte eingegangen wird, die im Rahmen dieses Projekts zu analysieren sind, sollen die Begriffe ‚Identifikation' und ‚Authentifizierung' definiert werden:

- **Identifikation** ist die Erkennung einer Einheit wie z. B. einer bestimmten Person. Identität ist definiert als "a reference or designation used to distinguish a unique and particular individual (organization or device)" (Bouma 2006; Deutsche Emissionshandelsstelle im Umweltbundesamt 2010b, 1).
- **Authentifizierung** ist der Prozess, durch den die elektronische Identität eines Nutzers mithilfe eines Informationssystems für einen bestimmten Anlass bestätigt und validiert wird. Die Au-

thentifizierung kann auch mithilfe eines Passworts oder Biometrie gewährleisten, dass der Nutzer der wahre Besitzer dieses Berechtigungsnachweises ist (UK Cabinet Office 2002, 4).

Dabei sind zwei Typen der Authentifizierung zu unterscheiden (Price 2008, 95-103):

(1) **unilaterale Authentifizierung**, bei der nur eine Partei die andere von ihrer Identität überzeugt, aber nicht umgekehrt. Sie ist auch als einseitige Authentifizierung bekannt.
(2) **bilaterale Authentifizierung**, bei der sich jede Partei zur selben Zeit von der Identität der jeweils anderen Partei überzeugt. Sie wird auch als gegenseitige Authentifizierung bezeichnet.

1.2. Zielsetzung der Studie

Die Zielsetzung des Forschungsvorhabens ist es, Einführungskonzepte für IT-Infrastrukturprojekte am Beispiel des nPA bzw. der AusweisApp zu differenzieren und zu bewerten. Im Rahmen des Projektes eKIT werden die Anforderungen der relevanten Akteure analysiert, die Kommunikation verschiedener Anwendungsfälle untersucht, und konkrete Gestaltungsempfehlungen für weitere Infrastrukturprojekte am Beispiel des nPA bzw. der AusweisApp entwickelt.

Fokus des Projektes ist die sorgfältige Analyse des Marktpotenzials für den nPA/die AusweisApp, um klare Hinweise für die Strategieentwicklung hinsichtlich der lohnenden Anwendungsbereiche zu erhalten. Die Ergebnisse der Marktpotenzialanalyse ermöglichen eine Betrachtung der Aufnahmefähigkeit des Marktes sowie auch der Anwendungsbereiche des nPA.

Die Verfügbarkeit der Infrastruktur ist einer der wichtigsten Faktoren für den Erfolg des elektronischen Identitätsmanagements. Die Förderung dieser Infrastruktur setzt den Einsatz entsprechender Geschäftsmodelle voraus, die eine einfache und kostengünstige Beschaffung der Produkte für die Bürger ermöglichen. Ziel der Studie ist es deshalb, zu ermitteln, wie und durch welche Geschäftsmodelle die AusweisApp für die Endnutzer verfügbar werden kann. Dazu werden beteiligte Akteure und Einflussfaktoren in diesem Bereich identifiziert und organisationsübergreifende Modelle für den nPA/die AusweisApp entwickelt.

Für die Auseinandersetzung mit den genannten Aspekten ist es neben der Grundlagenarbeit auf Basis einer Literaturauswertung und Dokumentenanalyse notwendig, die involvierten Akteure in Form von Expertengesprächen einzubinden. Abbildung 1 stellt die Komponenten des Projekts und ihre Zusammenhänge vor. Die entwickelten Modelle (u. a. Modelle des Vertrauens und der Einfachheit) werden in einer empirischen Phase überprüft. Die Ergebnisse fließen in die Überprüfung von Marktchancen und die Entwicklung möglicher Kommunikationsstrategien ein. Marktchancen und Kommunikation stehen in enger Beziehung. Mit einer geeigneten Kommunikation können die Markteinführungsmodelle erfolgreich gestaltet und die Marktchancen des nPA/der AusweisApp gesteigert werden. Einfachheit und Vertrauen stehen wiederum im Mittelpunkt sowohl hinsichtlich der Marktchancen als auch der

Kommunikation. Einfachheit und Vertrauen beeinflussen die Anwenderakzeptanz im Rahmen der technischen Implementationen. Daher müssen diese Aspekte den Anwendern effektiv vermittelt werden. Aus den gewonnenen Erkenntnissen werden Gestaltungsempfehlungen für IT Infrastrukturprojekte am Beispiel des nPA/der AusweisApp abgeleitet.

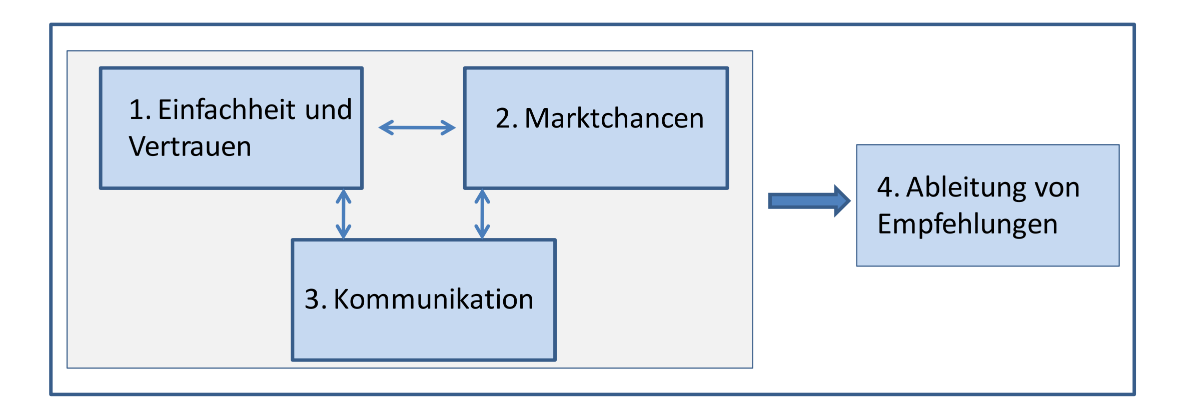


Abbildung 1: Komponenten des Projektes

Anknüpfend an diese Herausforderungen brachten der Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München und das Institut für Medien- und Kommunikationsmanagement der Universität St. Gallen ihre Kompetenzen im Bereich Einfachheit und Vertrauen, Marktchancen und Kommunikation ein. Die Komponenten des Projektes und seine Phasen werden in einer Matrix in Abbildung 2 dargestellt. Für jede Komponente und Phase des Projektes werden auch die verantwortlichen Projektpartner aufgeführt.

Komponenten / Phasen	1. Einfachheit und Vertrauen	2. Marktchancen	3. Kommunikation	4. Ableitung von Empfehlungen
Konzept Entwicklung	TUM, Uni. St. Gallen	TUM	Uni. St. Gallen	TUM, Uni. St. Gallen
Empirische Validierung	TUM, Uni. St. Gallen	TUM	Uni. St. Gallen	TUM, Uni. St. Gallen
Auswertung und Empfehlungen	TUM, Uni. St. Gallen	TUM	Uni. St. Gallen	TUM, Uni. St. Gallen

Abbildung 2: Phasen und Komponenten Mapping und ihre verantwortlichen Projektpartner

1.3. Methodik

Die Studie basiert auf einer umfangreichen Literatur- und Internetrecherche. Nach Analyse der relevanten Dokumente wurden Randbedingungen, wie eID-Akteure in Europa, Geschäftsmodelle und Marktchancen abgeleitet/festgelegt. Vorstellungen der Nutzer konnten mithilfe einer Umfrage im Auftrag von D21, durchgeführt von TNS Infratest in Zusammenarbeit mit der Technischen Universität München, identifiziert werden. Daten und Informationen hinsichtlich der Anwendungsszenarien konnten anhand von Interviews mit jeweils einem Ansprechpartner der beteiligten Parteien herausgefunden werden. Folgende Forschungsfragen lagen dem Projekt zu Grunde und sollen in diesem Bericht adressiert werden:

1. FF: Welche Faktoren beeinflussen die Akzeptanz von eID-Infrastrukturprojekten?
2. FF: Welche Anforderungen werden von den involvierten Akteuren an eID-Projekte gestellt?
3. FF: Welche Aspekte hinsichtlich Vertrauen und Kommunikation sind bei der Einführung von eID-Projekten wichtig/zu berücksichtigen?
4. FF: Wie sieht das Marktpotenzial für die AusweisApp aus?
5. FF: Welche Einführungskonzepte für Infrastrukturprojekte am Beispiel des nPA/ der AusweisApp existieren?
6. FF: Welches Geschäftsmodell ist für die Einführung von eID-Projekten passend?
7. FF: Welche Kommunikationsstrategien der Einführung von eID-Projekten lassen sich differenzieren?
8. FF: Welche konkreten Handlungsempfehlungen lassen sich für weitere eID Infrastrukturprojekte ableiten?

1.4. Aufbau des Dokuments

Das vorliegende Dokument stellt den Abschlussbericht zum Projekt „Einführungs- und Kommunikationsstrategien für IT Infrastrukturprojekte“ (eKIT) dar. Ausgangspunkt dieser Studie ist die Erfassung der Umfeldvoraussetzungen für eID-Infrastrukturprojekte in Kapitel 2. Darin wird auf Faktoren, die die Akzeptanz von eID-Projekten beeinflussen, wie Nutzer- und Innovations-Charakteristika, und kritische Erfolgsfaktoren zur Akzeptanzförderung von eID-Projekten eingegangen. Kapitel 3 bietet einen Überblick über eID-Projekte in Europa und leitet Schlussfolgerungen hinsichtlich der Marktpotentiale solcher Projekte ab.

In Kapitel 4 werden die Marktchancen für eID-Infrastrukturen in Deutschland erläutert. Zunächst wird auf das Vorgehen zur Ermittlung von Marktchancen eingegangen. Danach wird eine Marktanalyse für die Einführung des nPA in Deutschland vorgestellt, die zentrale Marktcharakteristika der eID-Infrastrukturen in Deutschland beschreibt. Nachdem eID-basierte Geschäftsmodelle und Einführungsmodelle für eID-Infrastrukturen dargestellt wurden, werden ausgewählte eID-

Anwendungsszenarien beschrieben und analysiert. In Kapitel 5 werden Kommunikationsstrategien für die Einführung von eID-Infrastrukturprojekte in Deutschland differenziert und basierend auf den zuvor identifizierten Einflussfaktoren auf die Nutzerakzeptanz analysiert.

Der Abschlussbericht wird mit einer Zusammenfassung und Handlungsempfehlungen hinsichtlich Markteinführungs- und Kommunikationsstrategien für eID-Infrastrukturen in Kapitel 6 abgerundet. Darin werden die wesentlichen Erkenntnisse der Studie nochmals aufgegriffen und Handlungsempfehlungen vorgeschlagen.

2. Umfeldvoraussetzungen von eID-Infrastrukturprojekten

2.1. Einleitung

Die Adoption des neuen Personalausweises unterscheidet sich von den Adoptionsprozessen, die bei der Markteinführung anderer neuer Produkte stattfinden. Im Unterschied zu den dargestellten fünf Kriterien der Diffusion liegt bei der Adoption des nPA die Entscheidung zur Übernahme nicht bei der Adoptionseinheit, den Bürgern. Nach dem Personalausweisgesetz (PersAusG) müssen sich deutsche Staatsangehörige mit der Vollendung des sechzehnten Lebensjahres durch einen Personalausweis oder Reisepass ausweisen können (Bundesministerium der Justiz 2010a). Die Entscheidungsphase wird somit durch Gesetze des Staates geprägt. Rogers nennt solche Entscheidungssituationen „authority innovation decisions“ – Nutzer der Innovation haben wenig Einfluss bei der Übernahme der Innovation, diese wird von einer kleinen Gruppe beschlossen: „An individual member of the system has little or no influence in the authority innovation decision; he or she simply implements the decision once it is made by an authority“ (Rogers 2005, 29). „Authority“ Innovationsentscheidungen zeichnen sich durch eine hohe Adoptionsrate (die relative Geschwindigkeit, mit der die Mitglieder eines sozialen Systems diese Innovation annehmen) aus, insbesondere im Vergleich zu den zwei weiteren von Rogers vorgestellten Möglichkeiten der Adoption – die optionale („optional“) und kollektive („collective“) Entscheidungssituation. Die hohe Adoptionsrate wird aber weitgehend von den Besonderheiten der Entscheidungssituation und nicht von der subjektiven Einstellung der Adoptionseinheit gegenüber dem Produkt („perceived attributes of innovation“ (Rogers 2005, 221) oder der wahrgenommenen Nützlichkeit beeinflusst. Eine Wahlfreiheit für Bürger bleibt allerdings hinsichtlich der Nutzung der eID- und der Signaturfunktion bestehen. Um Aussagen über die erfolgreiche Übernahme des nPA zu treffen reicht es nicht, sich auf die Entscheidungsphase und die damit verbundene Adoptionsrate zu konzentrieren. Die Akzeptanz des nPA beinhaltet nicht nur die erfolgreiche Adoption, sondern drückt sich maßgeblich in der kontinuierlichen Nutzung der neuen elektronischen Funktionen durch Bürger und Wirtschaftsakteure aus.

2.2. Faktoren, die die Akzeptanz von eID-Projekten beeinflussen

Sowohl Diffusion[2] als auch Adoption[3] und Akzeptanz hängen von zahlreichen Einflussfaktoren ab. Während Adoptionsfaktoren den Adoptionsprozess und die erhoffte Übernahme einer Innovation be-

[2] Unter Diffusion wird sowohl die zeitliche Ausbreitung einer Innovation als auch die individuelle Entscheidung zur Übernahme einer Innovation verstanden (Rogers 2005, 13).

einflussen, beeinflussen Akzeptanzfaktoren die wiederholte Nutzung einer Innovation. Gemeinsam können sie in innovations-, personen- und umweltbezogene Einflussfaktoren unterschieden werden (Kollmann 1998, 117ff). Unter umweltbezogenen Adoptionsfaktoren werden makroökonomische, technologische, politisch-rechtliche und soziokulturelle Faktoren verstanden (Weiber 1992, 7). Auf diese wird in diesem Projektbericht nicht vertieft eingegangen. Das Forschungsprojekt konzentriert sich auf Faktoren, die individuelle Entscheidungen beeinflussen, da eine Nutzung der eID- und Signaturfunktion von den individuellen Entscheidungen der Bürger abhängig sind.

Zielgruppen

Die umfangreichste Zielgruppe des nPA bilden deutsche Staatsangehörige (**Bürger/Konsumenten**), die bei elektronisch abgewickelten Transaktionen die Rolle des Bürgers (Nutzer von E-Government Dienstleistungen) oder des Konsumenten (Nutzer von E-Commerce Diensten) annehmen (Kaya 2009, 17f). Laut einer Studie von BITKOM hinsichtlich der Akzeptanz des neuen Personalausweises sind von Behörden angebotene Dienste im Internet die bevorzugte Anwendungsmöglichkeit des nPA. Weiterhin besteht ein Interesse der Bürger an der Nutzung des Personalausweises bei Online-Banking-Dienstleistungen (38 % der befragten Internetnutzer) und bei Online-Shopping (33 %) (o.V 2010, 11). Individuen unterschiedlicher Altersgruppen verursachen Schwankungen in der vorausgesagten Akzeptanz des nPA – während jüngere Bürger die Einführung begrüßen, wächst mit steigendem Alter die Skepsis gegenüber dem neuen Personalausweis. Die neuen elektronischen Funktionen sind weiterhin für online aktive Bürger attraktiver – Individuen, die sich bis jetzt von Kommunikation und Transaktion im Netz ferngehalten haben, müssen also zuerst als Onliner gewonnen werden (Schallbruch 2010, 214).

Eine weitere Zielgruppe ist die **Wirtschaft**. Vor dem Hintergrund steigender Onlineaktivität und dem Zuwachs von Online-Einkäufen („Sechs von zehn Deutschen kaufen im Internet ein", BITKOM 2010) ist die Sicherheit und Zuverlässigkeit für Dienstanbieter im E-Business von strategischer Bedeutung. Durch den Einsatz des neuen Personalausweises können diese den Identitätsdiebstahl erschweren und durch den damit verbundenen Aufbau von Vertrauen höheren Umsatz erzielen (Kaya 2009, 27).

Behörden sind staatliche Einrichtungen, die Aufgaben der **Verwaltung** zu erfüllen haben. Dies sind vor allem Dienstleistungen des Staates gegenüber den Bürgern (Kaya 2009, 22). Die derzeitigen Angebote der Verwaltung beschränken sich mit einigen Ausnahmen wie der elektronischen Einkommensteuererklärung (ELSTER-Online) auf Informationsangebote – Öffnungszeiten, Formulardownload, Serviceinformationen (Kaya 2009, 22). Mit der Einführung des nPA können E-Government Dienstleistungen ausgeweitet und dadurch Behörden von Routineaufgaben entlastet werden.

[3] Unter Adoption versteht man die konkrete Übernahme einer Innovation durch ein Individuum (Rogers 2005, 4ff).

Einflussfaktoren

Um die Akzeptanzwahrscheinlichkeit einer Innovation charakterisieren zu können, kann zwischen Intention und Disposition der Zielpersonen unterschieden werden. Unter Intention wird verstanden, dass die Zielpersonen gewisse Ziele verfolgen, für deren Erreichung eine Innovation mehr oder weniger hilfreich sein kann. Im Mittelpunkt stehen daher hier die Charakteristika der Innovation. Verschiedene theoretische Modelle differenzieren Innovationscharakteristika, darunter insbesondere der Adaptionsprozess nach Rogers, TAM[4] und UTAUT[5]. Charakteristika der Innovation, welche die Intention der Zielpersonen berühren, werden in Kapitel 2.2.1 behandelt.

Der zweite Baustein, aus dem die Akzeptanzwahrscheinlichkeit abgeleitet werden kann, ist die Disposition. Für die Disposition sind die Charakteristika der Nutzer, wie Umgebung, Rolle oder persönliche Merkmale ausschlaggebend. Sowohl Alter, Geschlecht oder Erfahrung, als auch die Aufwandserwartung, freiwillige Nutzung und soziale Einflussfaktoren spielen für die Disposition eine entscheidende Rolle. Auch demografische, soziografische und physiografische Merkmale der Nutzer sowie umweltbezogene Einflussgrößen, die durch die Eigenschaften des Marktes bestimmt werden, beeinflussen die Disposition (Hensel/Wirsam 2008, 24f). Dabei ist allgemein festzustellen, dass innovationsbezogene Faktoren mit weniger Aufwand erhoben und analysiert werden können, als die sozioökonomischen oder umweltspezifischen Einflussgrößen, insbesondere im Falle grosser, heterogener Zielgruppen, da sie mit dem innovativen Produkt (oder Dienstleistung) und dessen bekannten Eigenschaften zusammenhängen. Charakteristika der Nutzer und ihrer Situation, welche die Disposition der Zielpersonen beeinflussen, werden in Kapitel 2.2.2 behandelt

Abbildung 3 stellt das Zusammenwirken der Innovations- und Nutzercharakteristika grafisch dar. Demnach beeinflusst die Charakteristika der Innovation die Intention, die Nutzercharakteristika sind ausschlaggebend für die Disposition. Intention und Disposition ergeben gemeinsam die Akzeptanzwahrscheinlichkeit. Aussagen über Merkmale von Innovationen wie auch Zielgruppen sollten daher die Ableitungen von Schlussfolgerungen für die Akzeptanz von eID-Infrastrukturprojekten ermöglichen.

[4] Technology Acceptance Model (TAM) (Davis 1989)
[5] Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003)

Abbildung 3: Das Zusammenwirken von Innovations- und Nutzercharakteristika (Quelle: Eigene Darstellung)

2.2.1. Innovationsbezogene Einflussfaktoren

Innovationsbezogene Faktoren beschreiben vor allem Charakteristika einer Innovation. Es finden sich hier also die wesentlichen Eigenschaften, die eine Innovation haben muss, um sich schnell auszubreiten. Rogers definiert fünf innovationsbezogene Faktoren: relativer Vorteil, Kompatibilität, Komplexität, Erprobbarkeit und Beobachtbarkeit (Rogers 2005, 15f). Diese haben neben anderen Variablen wie der Entscheidungssituation oder die Kommunikationskanäle den größten Einfluss auf die Adoptionsrate einer Innovation. Sie können auch für den Fall der Einführung des neuen Personalausweises herangezogen werden. Eine Innovation, die aus Sicht der potenziellen Nutzer mit ihren eigenen und den

Werten des sozialen Systems übereinstimmt, sehr vorteilhaft, gut beobachtbar und einfach zu verstehen ist sowie im kleinen Rahmen ausprobiert werden kann, wird schneller adoptiert (Rogers 2005, 16). Im Folgenden werden zunächst die Akzeptanzfaktoren nach Rogers, im Anschluss daran weitere Faktoren, die insbesondere auf die Einfachheit der Innovation abzielen, näher erläutert. Abgerundet wird dieses Unterkapitel mit Beispielen innovationsbezogener Faktoren.

2.2.1.1. *Akzeptanzfaktoren nach Rogers*

Relativer Vorteil

Der **relative Vorteil** (*relative advantage*) ist „(…) the degree to which an innovation is perceived as better than the idea it supersedes." (Rogers 2005, 15). Der relative Vorteil muss nicht immer ökonomischer Natur sein, sondern kann ebenso gut auch die soziale Akzeptanz oder das Ansehen verbessern. Umso größer der relative Vorteil einer Innovation ist, umso schneller breitet sie sich aus oder wird adoptiert.

Bei der Adoption einer Innovation, sowie bei deren späterer Akzeptanz durchläuft der potenzielle Nutzer komplexe Meinungsbildungsprozesse. Durch diese wird die Unsicherheit, die mit der Innovation verbunden ist, reduziert (Rogers 2005, 233). Die subjektiv wahrgenommene Vorteilhaftigkeit der Innovation hat dabei eine entscheidende Rolle für ihre Adoption und später ihre dauerhafte Bestätigung. Der relative Vorteil beschreibt das Ausmaß, in dem eine Innovation im Vergleich zu anderen Innovativen oder bisher verwendeten Produktalternativen die individuellen Bedürfnisse des Nachfragers besser befriedigen kann (Hensel/Wirsam 2008, 16). Im Fall des neuen Personalausweises muss folglich untersucht werden, inwieweit die neuen Funktionen den Nutzern einen erkennbaren Mehrwert bringen, damit diese einen Anreiz zur kontinuierlichen Benutzung verspüren.

Aus Sicht des Bürgers bietet die eID-Funktion den Vorteil einer einheitlichen Identität – dem Benutzer wird die mehrmalige Anmeldung bei verschiedenen Onlineanbietern von E-Government und E-Commerce Diensten erspart. Mit der Pseudonymfunktion kann sich der Bürger außerdem bei einem Dienstanbieter ohne Übermittlung personenbezogener Daten anmelden und wird bei wiederholtem Besuch der Website wieder erkannt (Schallbruch 2010, 216). Das reduziert den Aufwand bei Onlinetransaktionen deutlich. Im Vergleich zu der früheren Transaktionsabwicklung im Internet, wird für die Bürger die Sicherheit erhöht, indem die Geschäftspartner in einem Authentifizierungsprozess vor der eigentlichen Datenübermittlung ein Berechtigungszertifikat vorweisen müssen, um auf die personenbezogenen Daten des nPA zugreifen zu können (Bundesministerium des Inneren 2008, 85). Bürger können danach in der Anzeige der zu übertragenden Daten gemäß dem Berechtigungszertifikat durch Ankreuzen die Übertragung bestimmter Daten auch ablehnen, und müssen zusätzlich zu dem Einlesen der Chipkarte eine PIN-Eingabe zur Bestätigung des Datentransfers ausführen, d. h. sie haben die persönliche Wahl zur Weitergabe der Daten. Die Fälschungssicherheit des Vorgangs wird gesteigert,

indem statt der einzelnen Komponente „Wissen“ (PIN-Eingabe) die Kombination von „Wissen“ (Ausweis-PIN) mit physischem „Besitz“ (Ausweiskarte) etabliert wird. Die neuen Funktionen werden für Nutzer attraktiv sein, vorausgesetzt, dass durch deren Nutzung keine zusätzlichen Sicherheitsrisiken für Bürger entstehen. Als solche könnten z. B. der Kartendiebstahl oder die Entwendung von personenbezogenen Daten gesehen werden. Um missverstandene Sicherheitslücken oder Angst vor Datenmissbrauch zu verhindern, ist besonders wichtig, dass die Vorgänge im Rahmen der Onlineidentifizierung für den Benutzer transparent gemacht sind.

Die wahrgenommenen Vorteile der eID-Funktion des neuen Personalausweises hängen weiterhin maßgeblich von der Anzahl der Anwendungen in der Verwaltung und Wirtschaft ab, die den nPA als Identifizierungsmöglichkeit unterstützen werden (Schallbruch 2010, 212). Ist eine Vielzahl solcher Anwendungsmöglichkeiten vorhanden, wird Bürgern eine höhere Bequemlichkeit, Flexibilität und Verfügbarkeit von Verwaltungsleistungen angeboten (Bundesministerium des Inneren 2008, 30). Im Rahmen eines zentralen Anwendungstests wurden in Zusammenarbeit mit Akteuren aus der Wirtschaft attraktive Anwendungen für den nPA entwickelt. Ziel ist, dass Bürger bei der Einführung des nPA den Anreiz haben, diesen zu nutzen.

Für Behörden stellt der eindeutige Identitätsnachweis im Internet eine entscheidende Voraussetzung für die Verwaltungsmodernisierung und Grundlage zur Bereitstellung von innovativen Dienstleistungen im E-Government Bereich dar. Beispielszenarien sind die Ablösung des Meldeverfahrens bei Namens- oder Adressenänderung durch ein auszufüllendes Onlineformular, der Einsatz des nPA für die Einkommensteuererklärung, für Kfz-An- und Ummeldung sowie bei der Internetauskunft aus Registern und Datenbanken (Bundesministerium des Inneren 2008, 49f). Vorteile gegenüber der früheren Situation treten für alle Beteiligten auf. Es wird erhofft, dass durch die standardisierte eID-Funktion mehr Bürger die modernisierten Versionen von bisherigen Onlineangeboten (wie die Einkommenssteuererklärung) sowie die neu entstandenen Dienste (wie das Onlinemeldeverfahren) nutzen werden. Mit dem Einsatz der eID-Funktion sparen die Behörden Ressourcen z. B. durch den Verzicht auf die Belegpflicht oder die verkürzten Bearbeitungszeiten aufgrund der elektronischen Erfassung der Daten. Die eindeutige Identifizierungsmöglichkeit erlaubt somit die Ausbreitung des Serviceangebots der Verwaltung im Internet, führt zu Kosteneinsparungen und entlastet die Sachbearbeiter in den Behörden von Routineaufgaben (DIHK 2009, 14ff; Bundesamt für Sicherheit in der Informationstechnik 2005, 4).

Aus Sicht der teilnehmenden Wirtschaftsakteure ergeben sich ebenfalls Vorteile durch die Einführung der elektronischen Identitätsnachweisfunktion. Für Anbieter von Onlineleistungen, wie Online-Shopping und Online-Banking, steigt die Sicherheit, weil dem Identitätsdiebstahl (z. B. durch Phishing) durch die eindeutige Identitätsfunktion vorgebeugt wird. Der Aufbau von Zuverlässigkeit und Vertrauen beim Konsumenten durch die eingesetzten Sicherheitsmechanismen im Onlinehandel kann weiterhin zu steigenden Nutzerzahlen und erhöhtem Umsatz führen. Im Online-Banking, wo das

Vertrauen der Kunden von besonderer Bedeutung ist, kann durch den Einsatz der eID-Funktion zusätzlich zu den bestehenden PIN-TAN-Verfahren die Sicherheit erhöht und neue Funktionen wie z. B. die medienbruchfreie Online-Kontoeröffnung ermöglicht werden (Bundesministerium des Inneren 2008, 45f). Allerdings sollte das Basislesegerät nicht für sensible Transaktionen verwendet werden, da es nicht sicher genug ist. Durch die Verwendung von Lesegeräten höherer Sicherheitsklassen können Transaktionen sicher abgewickelt werden, auch wenn der Rechner durch Schad-Software angegriffen wird (Euro Security 2010). Der nPA kann im Rahmen von Online-Banking sicher eingesetzt werden, wird aber die bestehenden PIN-TAN-Verfahren wohl nicht ersetzen, obwohl er eine alternative Abwicklungsform anbietet. Online-Banking beinhaltet zwei Komponenten: Identifikation und Autorisierung. Die Identifikation kann durch eine PIN-Nummer oder über den nPA geschehen, wobei die Verwendung des nPA hierfür als sicherer angesehen wird. Eine Autorisierung wird nicht mehr wie bisher, mittels TAN-Nummern erreicht, sondern durch die qualifizierte elektronische Unterschrift (Euro Security 2010). Allerdings stellen die derzeit angebotenen TAN-Verfahren aus Sicht der Banken eine ausreichend sichere Authentifizierungsmöglichkeit dar, weshalb es derzeit nicht geplant ist, den nPA im Online-Banking einzusetzen (Borchers 2010b; Euro Security 2010). Laut Bankexperten lässt sich außerdem das häufigste Nutzungsszenario – Online-Banking vom Arbeitsplatz aus – nicht mit dem nPA realisieren. Kartenlesegeräte und AusweisApp können aufgrund der Sicherheitsrichtlinien der Unternehmen am Arbeitsplatz nicht installiert daher nicht genutzt werden. Analog zu den sich ergebenden Vorteilen in der Verwaltung können auch in der Privatwirtschaft Kosteneinsparungen realisiert werden, indem Geschäftsprozesse vollständig elektronisch abgewickelt werden. Teilnehmende Wirtschaftsakteure können sich weiterhin gegenüber Konkurrenten durch die erhöhte Sicherheit und Zuverlässigkeit ihrer Angebote strategische Wettbewerbsvorteile sichern und ihr Markenimage stärken.

Neben der elektronischen Identitätsnachweisfunktion bietet der nPA auch eine optionale elektronische Signatur, für die der Bürger bei einem Zertifizierungsanbieter ein Signaturzertifikat abfragen muss (Bundesministerium des Inneren 2008, 93). Die Übernahme der optionalen Funktion einer qualifizierten elektronischen Signatur hat den Charakter einer vorbeugenden Innovation – Nutzer entscheiden sich gegen die Ausführung von Onlinetransaktionen ohne eine zusätzliche Signatur um zukünftige Risiken bei deren Abwicklung zu minimieren (Roßnagel 2006, 75). Solche Innovationen werden von Rogers als „preventive innovations" bezeichnet und haben in der Regel eine unsichere Adoptionsrate im Vergleich zu anderen Innovationen, da die Vorteile der Adoption erst in der Zukunft eintreten oder überhaupt nicht zu beobachten sind (Rogers 2005, 233). Die subjektiv wahrgenommenen Vorteile für Bürger und Wirtschaft hängen deswegen stark von den entwickelten Anwendungen für die Signatur ab – sind attraktive Anwendungsmöglichkeiten vorgesehen, so steigt die Akzeptanz der Technologie. Eine bereits existierende und erfolgreich verwendete Einsatzmöglichkeit ist die Unterschriftfunktion im elektronischen Abfallnachweisverfahren. Analog zu der eID-Funktion spielt hier die Transparenz auch eine wichtige Rolle – den Nutzern muss erklärt werden, welche Rechtsfolgen die Nutzung der elektronischen Signatur nach sich zieht, um die Unsicherheit zu reduzieren.

Kompatibilität

Kompatibilität (*compatibility*) ist „(…) the degree to which an innovation is perceived as being consistent with existing values, past experiences, and needs of potential adopters.“ (Rogers 2005, 15). Die Kompatibilität einer Innovation beinhaltet, inwieweit die Neuerung in die technische Infrastruktur der Adoptionseinheit passt sowie die Vereinbarkeit dieser mit bestehenden Werten, Normen und Bedürfnissen (Hensel/Wirsam 2008, 16). Im Fall des nPA stellt der erste Aspekt – die Vorbereitung der technisch-organisatorischen Rahmenbedingungen bei den einzelnen Nutzern eine noch zu bewältigende Herausforderung dar (Schallbruch 2010, 213). Für die Nutzung der eID-Funktion brauchen Bürger ein Lesegerät, das für Karten mit kontaktloser Schnittstelle geeignet ist, einen internetfähigen Rechner und eine Treiber-Software, die auf dem Rechner installiert ist. Für die elektronische Signatur wird ein Komfortlesegerät mit eigenem Display und einem separaten Tastaturfeld ("PIN-Pad") zur Eingabe der Signatur-PIN benötigt (Bundesministerium des Inneren 2010c). Für die reibungslose Nutzung der digitalen Funktionen wird von der Bundesregierung die Verfügbarkeit von Lesegeräten durch den Verkauf und Vertrieb von IT-Sicherheitskits gefördert. Für den Aufbau der technischen Infrastruktur beim Nutzer werden Chipkartenleser, Informationen zur Nutzung von Chipkarten sowie weitere individuell zusammengestellte Bestandteile kostenlos oder verbilligt ausgegeben (Bundesministerium des Inneren 2010c). Durch Kooperation mit unterschiedlichen Anbietern wie Volksbanken, Krankenversicherungsanbietern sowie Zeitschriften werden den Kunden von den entsprechenden Partnerunternehmen unentgeltliche oder verbilligte IT-Sicherheitskits angeboten und somit der Aufbau einer technologischen Infrastruktur bei den Bürgern wie auch bei den teilnehmenden Wirtschaftsakteuren gefördert (Die Beauftragte der Bundesregierung für Informationstechnik 2010). Solche Maßnahmen haben einen positiven Einfluss auf die Kompatibilität und dadurch auf die Akzeptanz der elektronischen Funktionen des neuen Personalausweises bei den Nutzern.

Umso besser sich eine Innovation an bestehende Werte und Erfahrungen des sozialen Systems oder eines Individuums anpasst, umso eher wird diese Innovation auch adoptiert, da ein Individuum bei der Adoption einer inkompatiblen Innovation ein hohes soziales Risiko eingeht. Da sich soziale Werte nur sehr langsam ändern, dauert es – wenn überhaupt - sehr lange, bis eine inkompatible Innovation übernommen wird (Rogers 2005, 16).

Komplexität

Der Grad der **Komplexität** (*complexity*) bezeichnet, wie schwer eine Innovation zu verstehen ist (Rogers 2005, 16). Da jedes Individuum einen unterschiedlichen Wissensstand hat, scheint dieser Faktor zuerst sehr individuell. Während dies bei sehr technischen Innovationen auch zutrifft und durchaus auch ein Kriterium sein kann, wird hier vor allem der allgemeine Wissensstand des sozialen Systems betrachtet. So sind die Bürger der Bundesrepublik zum Beispiel mit der Nutzung eines Computers relativ vertraut, während für abgelegene Indianerstämme Lateinamerikas die Nutzung eines Computers

sehr schwierig bzw. komplex erscheinen kann. Je komplexer eine Innovation also ist, umso länger dauert es, bis eine Innovation adoptiert wird (Rogers 2005, 16).

Rogers bewertet die Komplexität, Erprobbarkeit und Kommunizierbarkeit im Vergleich zu den oben bereits dargestellten relativer Vorteil und Kompatibilität als weniger relevante Einflüsse auf die Adoptionsrate (Rogers 2005, 95). Die Komplexität einer Innovation beinhaltet ihre Nutzbarkeit sowie die Schwierigkeiten beim Erlernen und Erkennen des Nutzens der Innovation. Beim nPA drückt sich die wahrgenommene Komplexität vor allem in der Erlernbarkeit der neuen Funktionen aus – die eID-Funktion und elektronische Signatur.

In einem Positionspapier von BITKOM werden dazu zahlreiche Empfehlungen gemacht: Es soll eine einfache verständliche Benutzerführung zur Verfügung gestellt werden, die sich an bestehenden grafischen Oberflächen orientiert und interaktiv gestaltet ist, um die schnelle Erlernbarkeit zu fördern (BITKOM 2009, 2). Nutzer sollen durch die Bereitstellung von Supportfunktionen unterstützt werden – Help Desk, Webseiten, Informationsmaterialien u. a. (Bundesministerium des Inneren 2008, 82). Besonders wichtig ist die Schaffung von Transparenz durch die Implementierung eines guten Sperrmanagements und die Einrichtung eines zentralen Ansprechpartners, an den sich Bürger mit Fragen zur Sperrung des nPA, bei Verlust oder Diebstahl wenden können. Die relativ hohe Komplexität der Sicherheitstechnologien des nPA wirkt sich jedoch nicht unbedingt negativ auf seine Akzeptanz aus. Nutzer brauchen kein umfassendes technologisches Verständnis zu haben, um die Sicherheit des nPA als hoch einzuschätzen – zum Beispiel werden Geldautomaten weitgehend benutzt, obwohl Nutzer wenig über die darin implementierten Sicherheitsmechanismen wissen (Roßnagel 2006, 77).

Erprobbarkeit

Mit **Erprobbarkeit** (*trialability*) wird „(…) the degree to which an innovation may be experimented with on a limited basis.“ (Rogers 2005, 16) bezeichnet. Dieses Kriterium ist besonders für die Nutzerkategorien der Innovatoren und frühen Adopter wichtig, da sie nur sehr beschränkt auf Informationen anderer zurückgreifen können und somit ein hohes Risiko bei der Adoption eingehen. Ist es daher möglich, die Innovation im kleinen Rahmen zu testen, sind die möglichen negativen Konsequenzen beschränkt, und die Innovation wird eher ausprobiert und eventuell adoptiert.

Während des Adoptionsprozesses sowie nach der Adoption der Innovation sammeln Individuen Informationen über die Innovation, wägen die Vorteile gegenüber ihren Nachteilen ab, bewerten die Benutzerfreundlichkeit und die Möglichkeiten zur Einbindung der Neuerung in die individuellen Abläufen mit dem Ziel, die Unsicherheit der Innovation zu reduzieren. Innovationen, die leicht erprobbar sind, sind mit geringerer Unsicherheit für die Nutzer verbunden – Neuerungen, die mit wenig Aufwand getestet werden können, haben folglich eine höhere Adoptionsrate (Hensel/Wirsam 2008, 24). Da die Adoptionsentscheidung beim nPA autoritär ist und keine Möglichkeit für jeden einzelnen Bürger vorgesehen, ist zuerst die Funktionen des nPA zu testen und diese erst dann zu übernehmen, könn-

te man schlussfolgern, dass der nPA nicht erprobbar ist. Dennoch ist es möglich, Aussagen über die Akzeptanz des nPA anhand eines Testkonzepts zu machen – seit Oktober 2009 laufen Test- und Implementierungsmaßnahmen. In einem zentralen Anwendungstest werden unterschiedliche E-Business- und E-Government-Dienste in Zusammenarbeit mit Dienstanbietern unterschiedlicher Branchen vorbereitet (o. V. 2009b, 5). Teilnehmende Bürger sind dabei Kunden der beteiligten Wirtschaftsakteure. Ziel des zentralen Anwendungstests, der von einem Kompetenzzentrum im Auftrag des BMI (Bundesministerium des Inneren) unterstützt wird, war die Bewertung der Praxistauglichkeit, Handhabbarkeit und Akzeptanz des nPA und die Entwicklung attraktiver Applikationen für die Funktionen des nPA vor seiner Einführung im November 2010 (o. V. 2009b, 5). Die gesammelten Ergebnisse könnten erste Informationen über die Akzeptanz des nPA bieten.

Kommunizierbarkeit/Beobachtbarkeit

Der letzte innovationsbezogene Faktor ist die **Beobachtbarkeit** (*observability*), welche Rogers als „(…) the degree to which the results of an innovation are visible to others.“ (Rogers 2005, 16) definiert. Wenn Ergebnisse einer Innovation für andere gut sichtbar sind, erfahren diese entweder von der Innovation oder fragen den Adopter nach Erfahrungen. Ist eine Innovation gut beobachtbar, breiten sich Informationen über diese Innovation schneller aus.

Der Begriff Kommunizierbarkeit bezeichnet, inwieweit man Nutzern die Eigenschaften oder den Nutzen der Innovation bekannt machen kann (Hensel/Wirsam 2008, 24). Je größer die Beobachtbarkeit der Innovation, desto schneller ist in der Regel deren Adoption. Im Fall der nPA-Einführung bekommen Nutzer (Bürger, Wirtschaft, Verwaltung) die Möglichkeit, die Eigenschaften des nPA selber zu „beobachten“ – aber erst nachdem sie diesen erhalten und eingesetzt (sich für die Adoption entschieden) haben. Für die Akzeptanz sind also die individuellen Erfahrungen im Umgang mit dem nPA sowie die allgemeine Informiertheit der Nutzer über die Eigenschaften des nPA ausschlaggebend.

2.2.1.2. *Beispiele innovationsbezogener Faktoren*

Im folgenden Abschnitt werden innovationsbezogene Faktoren, wie Biometrie, Authentifizierungsmethoden sowie Ergonomie und Einfachheit näher betrachtet. Der relative Vorteil dieser Faktoren besteht darin, dass sie Neuerungen darstellen, die wesentliche Vorteile zu bestehenden Authentifizierungsmethoden bspw. über Passworte bieten. Kompatibilität besteht darin, dass Werte, Erfahrungen und potenzielle Erwartungen von Bürgern in die Entwicklung neuer Authentifizierungsmethoden miteinfließen. Für die Adoption der folgenden Authentifizierungsmethoden ist es vor allem wichtig, dass deren Komplexität für Bürger minimiert wird, da dann eine bessere Akzeptanz erzielt werden kann. Erprobbarkeit und Beobachtbarkeit sind Aspekte, die an dieser Stelle zu vernachlässigen sind, da zwar Anwendungstests im Vorfeld stattgefunden haben, allerdings nur ausgewählte Bürger daran teilnehmen konnten.

Biometrie

Biometrie ist eines der am heftigsten diskutierten Merkmale eines digitalen Ausweises. Ein Vorteil der biometrischen Verfahren ist ihre Sicherheit. Des Weiteren reduziert sich dadurch das Risiko, dass Passwörter oder PIN-Nummern vergessen oder gestohlen werden können. Auf der anderen Seite entstehen durch Missbrauch erhebliche Konsequenzen. Werden biometrische Daten gestohlen, ist es nicht möglich, diese zu ändern, wie dies bei Passwörtern der Fall ist.

Auch wenn es Meinungen (Dunstone 2000) gibt, wonach die Speicherung biometrischer Daten nicht gefährlich ist, haben Bürger hauptsächlich hinsichtlich der Wahrung ihrer Privatsphäre Bedenken. Aufgrund dessen entstehen hitzige Diskussionen, viele Bürger betrachten die Biometrie weiterhin als ein umstrittenes Thema. Immer mehr Bürger sehen ihre Privatsphäre durch Biometrie bedroht, da diese es der Regierung und anderen Organisationen ermöglichen könnte, unbemerkt persönliche Merkmale wie auch die gesundheitliche Verfassung zu überwachen. Die Speicherung von zwei Fingerabdrücken ist beim nPA optional, während dies für den elektronischen Reisepass (ePASS) in Deutschland verpflichtend ist. In den Medien wurde diskutiert, ob die Speicherung das Grundrecht zur informationellen Selbstbestimmung verletzt, da die Daten ohne Kontrolle des Eigentümers übertragen werden und „niemand weiß, wer Zugriff darauf hat“ (Chaos Computer Club e.V.). Von der deutschen Regierung wurde ausdrücklich erklärt, dass nur Regierungsbeamte Zugang zu den biometrischen Daten erhalten.

Der Hauptunterschied des nPA zum ePASS ist, dass das Hinzufügen von biometrischen Daten optional ist und Ausweisbesitzer entscheiden können, ob biometrische Daten hinzugefügt werden sollen. Falls diese vorhanden sind, kann der nPA innerhalb der Schengenländer als Reisedokument verwendet werden.

Das Hinzufügen von biometrischen Daten zu den nationalen Identifikationsdokumenten musste von allen EU-Mitgliedsstaaten als Teil der European Citizen Card (ECC) umgesetzt werden. Verschiedene Länder haben dies bereits eingeführt. In den meisten Ländern wurden diese Ausweise von Bürgern problemlos akzeptiert. Die anhaltende Diskussion und negative Haltung der deutschen Bürger kann in Onlineforen und Blogs zum Thema nPA verfolgt werden. Dies ist ebenfalls ein Beweis für den grossen Einfluss kultureller Unterschiede auf die Einführung einer neuen Technologie.

Authentifizierungsmethoden

In der Literatur werden verschiedene Möglichkeiten zur Identifikation von Personen definiert. Tabelle 1 listet die verschiedenen Möglichkeit in Anlehnung an Clarke auf (1994, 6ff):

Möglichkeiten der Identifikation	Clarkes Definition	Beispiele
Erscheinung	Wie die Person aussieht	Nutzung von Fotos auf Ausweisdokumenten, Gesichtsbiometrie
Soziales Verhalten	Wie die Person mit anderen interagiert	Ausbildungsnachweise, Mobilfunk Aufzeichnungen
Namen/Codes	Wie die Person von anderen oder einer Organisation genannt wird	Name, der im Einwohnermeldeamt steht, Geburtsurkunde, Ausweisnummer, Sozialversicherungsnummer, usw.
Wissen	Was die Person weiß	Passwörter, PINs
Tokens	Was die Person hat	Smart Cards, Secure ID Cards
Bio-Dynamik	Was die Person tut oder ist	Die meisten Formen der Biometrie: Fingerabdrücke, Iris, Retina, usw.
Oktroyierte, physikalische Merkmale	Was die Person jetzt ist	Größe, Gewicht

Tabelle 1: Verschiedene Authentifizierungsmethoden (Clarke 1994)

Im Allgemeinen kann man diese verschiedenen Identifikationsfaktoren zu drei Schutzmethoden zusammenfassen (Petkovic/Jonker 1998, 1; o. V. 2010c, 90):

(1) Wissen, wie Passwörter, PINs oder persönliche Informationen (wie den Mädchennamen der Mutter),
(2) Besitz, Nutzung von Hardware-Sicherheits-Token, wie Chipkarten mit Sicherheitsmodul,
(3) Sein, biometrische Methoden, wie z. B. Gesichtsbild, Fingerabdrücke und Iris.

Nach heutigen Erfahrungen über die genannten Methoden zum Schutz von Identitäten wird der Schutz durch Wissen als nicht ausreichend eingeschätzt (o. V. 2010c, 90). Viele Organisationen sammeln bzw. speichern persönliche Informationen, wie z. B. den Mädchennamen der Mutter als Sicherheitsfrage. Diese Informationen können ebenfalls mithilfe einer Recherche über eine Person in Erfahrung gebracht werden. Das Problem mit Passwörtern ist ähnlich: Gewöhnlich tendieren Menschen zur Nutzung desselben Passworts bzw. einer Anzahl von wenigen Passwörtern für alle Authentifizierungsmechanismen um eine einfache Identifizierung sicherzustellen. Menschen können ihre Passwörter vergessen, was weitere Probleme hervorruft. Um dies zu vermeiden, werden Passwörter häufig notiert. Eine andere Methode ist die Wahl von Passwörtern, an die man sich leicht erinnert, jedoch können diese auch leicht erraten werden. Einige Organisationen erlauben das Zurücksetzen eines Passworts telefo-

nisch oder nur mit einer Bestätigungs-E-Mail. Dies ist ein weiterer Nachteil von Passwörtern und persönlichen Informationen, den Nutzer normalerweise nicht erkennen.

Der Einsatz von biometrischen Methoden stößt schnell an rechtliche Grenzen bzw. verstößt gegen Datenschutzbestimmungen (o. V. 2010c, 90). Obwohl eine Authentifizierung mithilfe biometrischer Verfahren als sehr verlässlich angesehen wird, entstehen auch an dieser Stelle Probleme, da die Beständigkeit biometrischer Daten mit der Zeit variiert. Um dies zu berücksichtigen, beinhalten einige biometrische Authentifizierungssysteme eine Toleranzspanne. Jedoch vermindert dies die Zuverlässigkeit des Systems, da sich die Wahrscheinlichkeit einer falschen Akzeptanz erhöht. Obwohl die Verlässlichkeit von Biometrie als sehr hoch angesehen wird, gibt es in der Literatur Fälle, die Bedenken hervorrufen. Matsumoto et al. (2002) haben es geschafft 80 % der Fingerabdruckscanner mit falschen bzw. künstlichen Fingern zu täuschen (Matsumoto et al. 2002, 275ff). Bei diesem Experiment wurden künstliche Finger aus Gelatine benutzt. Diese wurden zu einem sehr hohen Anteil bestimmter Fingerabdruckscanner akzeptiert. Auch wenn es unwahrscheinlich ist, gibt es auch Fälle falscher Ablehnung bei einer biometrischen Authentifizierung. Das größte Risiko biometrischer Verfahren ist der Verlust. Einmal verloren oder kopiert ist die Identität des Nutzers das ganze Leben lang anfällig für missbräuchliche Verwendung. Die Zurückgewinnung ist nicht möglich, da biometrische Merkmale nicht wie Passwörter verändert werden können. Deshalb sind Angriffe gegen biometrische Verfahren gravierender als gegen andere Authentifizierungsschlüssel. Im Falle eines Angriffs auf eine zentrale Datenbank mit biometrischen Daten wären die Risiken katastrophal. Zudem werden für die biometrische Authentifizierung spezielle Lesegeräte benötigt. Zusätzlich sollten Schulungen sowohl für das Personal, das diese Technologie anwendet, als auch in einigen Fällen für Nutzer, eingeplant werden.

Aus den genannten Gründen stehen Hardware-Sicherheits-Token, in denen unter anderem Identitäten sicher gespeichert und verarbeitet werden, häufig mit kryptografischen Verfahren, im Mittelpunkt des Interesses. Trotz Erfahrungen mit derartigen Token in vielen Anwendungsbereichen sind Fragen nach der technischen Machbarkeit, der Wirtschaftlichkeit im praktischen Einsatz sowie rechtliche Fragen immer noch nicht vollständig geklärt (o. V. 2010c, 90). Authentifizierungsmethoden, die auf den Besitz eines Tokens basieren, leiden aber dennoch unter einer Vielzahl von Problemen. Sie können verloren, gestohlen oder sogar vervielfältigt werden. Für Online-Transaktionen benötigen Token die Installation spezieller Software und externer Lesegeräte, was zu einer Erhöhung der gesamten Kosten führt. Falls eine dieser Komponenten verloren geht oder beschädigt wird, kann sich der Nutzer nicht authentifizieren, bis diese ersetzt wird.

Es gibt auch Authentifizierungsmethoden, die aus einer Kombination der drei Faktoren bestehen. Dies wird als Multi-Faktoren-Authentifizierung bezeichnet. Die Nutzung von zwei gleichen Faktoren ist bei der Multi-Faktoren-Authentifizierung nicht erlaubt. Die Bereitstellung eines Passworts und des Mädchennamens der Mutter mag die Sicherheit leicht erhöhen, aber es ist immer noch eine Ein-Faktor-Authentifizierung. Bei der Zwei-Faktoren-Authentifizierung werden zwei Faktoren kombiniert, bspw.

wird für den Zugang zum Bankautomaten die Kombination aus Passwort und Bankkarte benötigt. Drei-Faktoren-Authentifizierungssysteme werden für den Zugang zu Sicherheitsbereichen genutzt. Die Stärke des Authentifizierungsschlüssels ist innerhalb einer Kategorie nicht kongruent. Ein zufällig gewähltes, achtstelliges, alphanumerisches Passwort wird voraussichtlich höhere Sicherheit bieten als der Mädchenname der Mutter. Im Allgemeinen ist die Sicherheit eines Systems höher, je mehr Authentifizierungsfaktoren genutzt werden. Jedoch gibt es hierbei auch Ausnahmen. Der Besitz einer Bankkarte und des dazugehörigen Passworts schützt den Nutzer wahrscheinlich nicht im selben Maße wie ein Gesichtserkennungssystem.

Auswahl der Multi-Faktoren-Authentifizierung

Wie bereits diskutiert, ist die Nutzung der Multi-Faktoren-Authentifizierung empfehlenswert. Die Wahl der Faktoren ist eine wichtige Entscheidung, die viele Aspekte wie Kosten, Zeit und Anwendbarkeit bzw. Relevanz beinhaltet. Die Regierung von Neuseeland betrachtete für die Wahl der richtigen Kombination bei ihren E-Government-Initiativen folgende Aspekte:

Aspekte	**Punkte, die zu beachten sind**
Bildungsniveau der Kunden	• Haben die Kunden die nötigen Fähigkeiten? • Stehen Trainingsmittel zur Verfügung? • Sind fortlaufende Schulungs- und Achtsamkeitsprogramme vorhanden?
Ressourcen für Kunden	• Haben die Kunden die nötige grundlegende Hard- und Software? • Ist es nötig, spezielle Software auf dem PC des Kunden zu installieren oder basiert das System darauf, dass Kunden über spezielle Hardware verfügen? • Soll das System mehrere Authentifizierungsschlüssel unterstützen, um alle Kunden abzudecken? • Wird angenommen, dass die EDV-Umgebung des Kunden mit schädlichen Programmen infiziert ist, oder dass übliche Computer-Schutzvorkehrungen vorhanden sind?
Andere (kundenbezogene) Aspekte	• Wie schwierig wird es sein, die Akzeptanz des Kunden zu erreichen? • Welche Möglichkeiten gibt es, um die Akzeptanz zu fördern? • Ist Portabilität eine Anforderung?
Mitarbeiterstab	• Welche Anforderungen werden an die Belegschaft für die Entwicklung und den fortlaufenden Betrieb des Systems gestellt? • Braucht die Belegschaft zusätzliches Training?
Systembetrieb	• Muss das System in bestehende Systeme integriert werden? • Was würde die Migration des bestehenden Systems beinhalten? • Welches Maß an Zuverlässigkeit muss erfüllt werden? • Kann das System angepasst werden, falls es notwendig wird? • Ist Kompatibilität mit anderen Systemen eine Anforderung? Falls ja, was wird verlangt? • Welche Zusammensetzung proprietärer und nicht proprietärer Technologie wird verwendet? • Systemangelegenheiten sind oft komplex, aber Vorrang sollte die Vision, die eine Organisation für ihr System hat, haben.
Systemkosten	• Was sind die Kosten für den Einsatz und den Betrieb des Systems? Diese sollten die Entwicklungs- und laufenden Betriebskosten beinhalten. Es werden auch Kosten anfallen um Sicherheitsvorschriften im Regierungssektor und andere Gesetze, Verordnungen und Standards einzuhalten.

Aspekte	Punkte, die zu beachten sind
Geschäftsbetrieb	• Können die Funktionen des Authentifizierungsschlüssels wirksam für die Geschäftsprozesse eingesetzt werden? Dies könnte der Treiber für die Auswahl eines Authentifizierungsschlüssels gegenüber anderen sein.
Anwendungszeitraum	• Gibt es zeitliche Einschränkungen für die Anwendung des Systems? Neue Lösungen brauchen länger, bis sie angewendet werden können.

Tabelle 2: Lösungsauswahlfaktoren (Information & Communications Technology branch)

Der Identifizierungsprozess des neuen Personalausweises läuft mithilfe einer PIN ab. Die Kombination aus Ausweis (etwas, das man besitzt) und PIN (etwas, das man weiß) gewährleistet höhere Sicherheit und somit doppelten Schutz. In den Medien wurden die Konsequenzen bei Verlust oder durch Ausspähen der PIN kritisiert (o. V. 2008). Das Risiko ist bei der Nutzung des nPA im Internet höher, da dort Nervosität oder eine abweichende Erscheinung vom Originalbild nicht nachgewiesen werden kann.

Ein Rechtsschutz für solch einen Fall wird offiziell nicht geplant. Bei Bankkarten kann der Kontobesitzer seine Karte ersetzen, falls die PIN verloren geht. Diese Möglichkeit und die Konsequenzen daraus sind im Gesetzesentwurf zum neuen Personalausweis nicht enthalten (Bundesregierung 2008).

Ergonomie und Einfachheit

Einfachheit ist ein weiterer entscheidender Erfolgsfaktor für digitale Ausweis-Projekte. Anders als andere Projekte, die zumeist eine spezielle Zielgruppe von Nutzern haben, betreffen solche landesweiten Projekte alle Bürger. Mit einem solch breiten Spektrum an Nutzern können Nutzeranforderungen nur mithilfe von repräsentativen Stichproben gewonnen werden. Angesichts der verschiedenen Hintergründe, technischen und sozialen Fähigkeiten der Bürger ist die Akzeptanz eines komplexen Systems eines der Hauptrisiken der Einführung. Um dies zu vermeiden, sollte das System so einfach wie möglich entworfen werden und die Nutzer sollten ein hohes Niveau an Unterstützung erhalten.

Die deutsche Bundesregierung hat die Entwicklung der AusweisApp für den neuen Personalausweis an ein Konsortium vergeben. Für den Erfolg des Projekts ist die Einfachheit der Software obligatorisch. Dies wird auch vom Konsortium als entscheidend anerkannt und entsprechend beachtet: „The Bürger-Client is Software for everyone and should be therefore easy-to-handle. We highly value the usability and accessibility in the development of our software“ (Open Limit 2009). Die AusweisApp wird auch im Rahmen von Testszenarien des Bundesministeriums des Inneren (BMI) getestet. Das BMI testete den nPA zusammen mit ungefähr 150 Organisationen anhand verschiedener Szenarien (Bundesministerium des Inneren 2009b). Die Teilnehmer hatten dabei die Möglichkeit, ihre Szenarien mit der AusweisApp ohne zusätzliche Kosten zu testen (o. V. 2009a). Die Ergebnisse dieser Tests können für die Einschätzung der Einfachheit der AusweisApp verwendet werden.

2.2.2.Personenbezogene Faktoren

Personenbezogene Einflussfaktoren der Akzeptanz umfassen nach Rogers drei Kategorien: sozioökonomischer Status, Persönlichkeitsmerkmale und Kommunikationsverhalten (Rogers 2005, 287). In der Adaptionsforschung wird dabei meist vertieft auf solche Faktoren eingegangen, die die Wahrnehmungen der Nutzer massgeblich prägen. Hierzu zählen das Vertrauen der Nutzer, ihre Risikowahrnehmung oder ihr Wunsch nach Sicherheit und Privatsphäre.

2.2.2.1. *Personenbezogenen Faktoren nach Rogers*

Zum **sozioökonomischen Status** (*socioeconomic status*) gehören Faktoren wie Bildung, sozialer Status und Einkommen (Rogers 2005, 288). Bei materiellen Innovationen (zum Beispiel Solarzellen) sind die Kosten für Innovatoren sehr hoch, sinken jedoch im Laufe der Zeit. Aber auch bei kostenlosen oder immateriellen Innovationen können bei der Anwendung später Kosten entstehen, die von den Individuen abgeschätzt werden.

Die Einstellung gegenüber Neuem, Neugierde, Spontanität, das Umgehen mit Risiko, die Einstellung zur Wissenschaft, Selbstbewusstsein und die Lernbereitschaft sind die wesentlichen Faktoren der **Persönlichkeitsmerkmale** (*personality values*) (Rogers 2005, 289f). So zeichnen Innovatoren zum Beispiel der bewusste Umgang mit Risiko und ein hohes Selbstbewusstsein aus, während Nachzügler Neuem gegenüber oft negativ eingestellt sind.

Unter **Kommunikationsverhalten** (*communication behavior*) versteht Rogers die Art der Kommunikation eines Individuums mit seiner sozialen Umgebung (Rogers 2005, 295f). Während Innovatoren stark in ihr weites soziales Netzwerk integriert sind und sich auch über Massenmedien informieren, haben Nachzügler meistens ein sehr kleines, lokales Netzwerk und agieren auch nur innerhalb dessen.

2.2.2.2. *Weitere bedeutende personenbezogene Faktoren*

Einer der wichtigsten Erfolgsfaktoren des nPA-Projekts ist dessen Akzeptanz durch die Endnutzer, die Bürger. Für die Akzeptanz des digitalen Ausweises ist der Aspekt ‚Vertrauen' von entscheidender Bedeutung. Bedenken hinsichtlich der Datensicherheit und dem Schutz der Privatsphäre können Nutzer davon abhalten, eine Innovation anzuwenden. Die Angst der Bürger, als blosse Nummer gesehen zu werden, ist ebenfalls Gegenstand der öffentlichen Debatte. Zahlreiche Vertrauensaspekte hängen außerdem von kulturellen Einflüssen ab. Des Weiteren beeinflusst auch die Bewertung der innovationsbezogenen Faktoren durch die Bürger deren Vertrauen. Auf den folgenden Seiten wird deshalb vertieft auf das Konstrukt Vertrauen sowie auf die Aspekte Sicherheit und Privatheit eingegangen.

Vertrauen

Unterschiedliche wissenschaftliche Disziplinen beschäftigen sich seit Jahrzehnten mit dem Vertrauenskonstrukt. Psychologen, Soziologen und auch Wirtschaftswissenschaftler sind aus unterschiedlichen Beweggründen daran interessiert, mehr über die Voraussetzungen und Wirkungen menschlichen Vertrauens zu erfahren. Aufgrund dieses interdisziplinären Interesses überrascht es kaum, dass keine allgemeingültige Definition von Vertrauen existiert. Trotzdem ist es wichtig, nach Gemeinsamkeiten der verschiedenen Forschungsstränge Ausschau zu halten. Vertrauen wird in der Literatur oft als subjektive Wahrnehmung beschrieben, eine Überzeugung, ein Glaube, ein Gefühl, und damit eine Eigenschaft, welche sowohl kognitive wie auch affektive Elemente beinhaltet (Belanger et al. 2002; Morgan/Hunt 1994; Lee/Turban 2001). Schewe und Nienaber definieren Vertrauen als „Erwartungshaltung eines Individuums gegenüber Individuen, Personengruppen oder Organisationen, dass diese sich in einem spezifischen und risikobehafteten Kontext zukünftig nicht opportunistisch verhalten“ (Schewe/Nienaber 2009, 230). Morgan und Hunt (1994) betonen, dass Vertrauen, verstanden als die Bereitschaft, eine Verwundbarkeit zu riskieren, Transaktionen erleichtert und stabile Geschäftsbeziehungen erst ermöglicht. Konsumenten müssen hinsichtlich der Integrität, der Kompetenz sowie auch des Wohlwollens der Geschäftspartner ein gewisses Vertrauensniveau erreichen, um sich an einer Transaktion zu beteiligen (Gefen 2000).

Wie aber sieht es im Bereich der computergestützten oder elektronischen Interaktion aus? Vertrauen im Netz unterscheidet sich von obigen Definitionen vor allem darin, dass das Vertrauensobjekt eine Website, also eine elektronische Benutzeroberfläche darstellt - im Gegensatz zu Individuen, Gruppen, physischen Produkten oder Objekten (Nissenbaum 2001). Dies impliziert, dass die Vielfalt der Hinweise zur Beurteilung der Vertrauenswürdigkeit eines Transaktionspartners beschränkt werden (Wang et al. 2004). Wir können also festhalten, dass Online-Vertrauen generiert wird, wenn der Nutzer, der Bürger oder der Konsument positive Eindrücke der Webpräsenz eines Transaktionspartners gesammelt hat und deshalb bereit ist, ein bestimmtes Maß möglicher Enttäuschungen in der Interaktion mit dem Geschäftspartner zu akzeptieren (Urban et al. 2009).

Verschiedene Applikationen des Internets (zum Beispiel Google Analytics) zeichnen Bewegungen der Nutzer, Mausklicks oder Suchanfragen auf, und speichern diese auf unbestimmte Zeit. Online-Transaktionen sind mit der Bereitstellung persönlicher Daten verbunden - unvermeidlich. Ein wesentlicher Bestandteil des Vertrauens im Netz ist somit die Bereitschaft der Nutzer ist, persönliche Daten zur Verfügung zu stellen (Schoenbachler/Gordon 2002). Diese Bereitschaft setzt den Nutzer einer gewissen Verwundbarkeit aus und löst dadurch Bedenken bezüglich des Schutzes dieser persönlichen Daten aus. Nutzer müssen sich im Rahmen einer Online-Transaktion entscheiden, ob der ihm versprochene Nutzen grösser ist, als das Risiko, das mit der Preisgabe der geforderten Daten verbunden ist.

Ziel von eGovernment Applikationen muss es sein, das potentielle Risiko für den Nutzer zu reduzieren und die Gewährleistung von Sicherheit und Privatheit zu kommunizieren. Zahlreiche Studien haben den Versuch unternommen, jene Einflussfaktoren zu identifizieren, die die Risikowahrnehmung im Internet reduzieren und Vertrauen erzeugen. So konnte gezeigt werden, dass nicht nur die Webpräsenz eines Anbieters Einfluss auf das Nutzervertrauen hat, sondern dass auch individuelle Persönlichkeitsfaktoren, wie etwa die Risikoneigung oder soziodemographische Faktoren, eine zentrale Rolle spielen. Vertrauen hängt außerdem von kulturellen Einflussfaktoren ab (Nasir et al. 2007, 1). Deshalb können Erfahrungen aus anderen Ländern nur bedingt auf Deutschland übertragen werden. Es ist auch so, dass Nutzer über die Zeit Vertrauen gegenüber gewissen grundlegenden Institutionen aufbauen, wie etwa dem Rechtsrahmen oder dem Medium Internet (Milne/Boza 1998; Olivero/Lunt 2004). Zusammenfassend kann festgehalten werden, dass Vertrauen auf einer Mikroebene von Eigenschaften des jeweiligen Individuums, auf einer Mesoebene von Eigenschaften des Interaktionspartners und schließlich auf einer Makroebene von Eigenschaften des kulturellen und institutionellen Kontextes beeinflusst wird.

Laut Schewe und Nienaber hat Vertrauen drei Hauptmerkmale: Erstens ist Vertrauen nötig, falls ein konkretes Risiko besteht. Adams definiert Risiko als "the probability of an adverse future event multiplied by its magnitude" (Adams 1995, 69). In der Verhaltensforschung ist man zu dem Schluss gekommen, dass das Verlangen nach Vertrauen nur in Gegenwart von Risiko und Verletzlichkeit auftritt. Bei E-Commerce Transaktionen wäre das Risiko z.B. der Diebstahl der Kreditkartendaten bzw. die Möglichkeit, das zugesicherte Produkt nicht zu erhalten. Das zweite Merkmal von Vertrauen ist seine Zukunftsorientierung. Vertrauen ist zukunftsorientiert, basiert aber auf vergangenen Erfahrungen. Menschen beurteilen das Risiko einer Situation subjektiv und können sich dafür entscheiden, das Risiko einzugehen, falls sie größere Vorteile für sich sehen. Das dritte Merkmal von Vertrauen ist die subjektive Beurteilung, die individuelle Wahrnehmung des Risikos. Es gibt einen Unterschied zwischen tatsächlichem und wahrgenommenem Risiko. Wahrgenommenes Risiko ist die subjektive Beurteilung des Menschen über die Existenz und Höhe eines Risikos. Verschiedene Theorien (wie z.B. die Perceived Risk Theory) befassen sich darauf aufbauend mit der Frage, wie Menschen Risiko wahrnehmen und daraufhin Entscheidungen treffen (Bauer 1967, 23-330).

Risikowahrnehmung: Privatsphäre und Sicherheit

Die Bereitschaft der Bürger, im Rahmen einer Transaktion persönliche Daten bereitzustellen und damit auch ein gewisses Risiko einzugehen, ist eine notwendige Voraussetzung für Online-Transaktionen wie auch E-Government-Angebote (Milne/Boza 1998; Eastlick et al. 2006). Risiken beziehen sich in der Wahrnehmung der Nutzer dabei vor allem auf die Privatheit und Sicherheit der persönlichen Daten. Die Forschung zeigt, dass die Wahrscheinlichkeit der Beteiligung an einer Online-Transaktion abnimmt, je höher die Besorgnis oder die Risikowahrnehmung der Nutzer ausfällt (Olivero/Lunt 2004; Phelps et al. 2000). Auch umgekehrt gilt: die Sorgen oder die Risikowahrnehmung nimmt ab, je mehr Vertrauen ein Nutzer hat - die Wahrscheinlichkeit, eine Transaktion durchzu-

führen, nimmt dann zu (Morgan/Hunt 1994; Milne/Boza 1998; Eastlick et al. 2006). Sicherheit und Privatheit sind also Treiber, welche einerseits auf Vertrauen und anderseits auf die Sorgen und Bedenken der Nutzer einzahlen, wie in Abbildung 4 dargestellt wird.

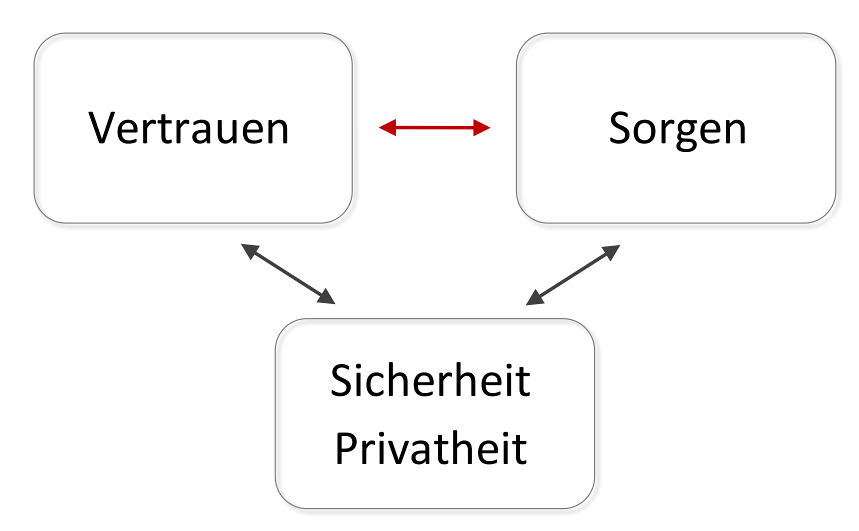


Abbildung 4: Abwägung von Vertrauen und Sorgen (eigene Darstellung)

Auf der einen Seite empfinden Menschen den Wunsch nach Privatheit, Abgeschiedenheit, Autonomie oder Selbstkontrolle, auf der anderen Seite wünschen sie sich jedoch den Austausch und möchten mit den Mitmenschen interagieren (Lanier/Saini 2008). Bezogen auf elektronische Interaktionen bedeutet dies vor allem, dass Bürger den Fluss und die Verbreitung ihrer Daten selber kontrollieren und steuern möchten, und insbesondere deren öffentliche Verfügbarkeit begrenzen. Die Definition von Privatsphäre nach Schoeman beinhaltet die Vertraulichkeit von Daten und allgemeinen Informationen über sich und seine persönlichen Merkmale: “A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life (…)” (Schoeman, 3). Diese Definition ist auch auf digitale Ausweise oder die eID zu übertragen, insbesondere wenn diese biometrische Komponenten umfasst. Das Hauptanliegen des Kartenbesitzers ist dann die Kontrolle darüber, welche Daten offengelegt werden und wer Zugriff auf sie hat. Besonders die geplante Speicherung von biometrischen Daten auf dem neuen Personalausweis weckt daher umgekehrt in der Bevölkerung Bedenken hinsichtlich des Datenschutzes (siehe Anhang C).

Ein weiterer Treiber der Risikowahrnehmung im Netz ist die Sorgen hinsichtlich einer unzureichenden Sicherheit (Belanger et al. 2002). Technische Systeme sind durch den Nutzer meist nicht beeinfluss- und kontrollierbar. Dabei können sie anfällig für technische Fehler, aber auch Eingriffe oder Manipulationen sein. Ist die Systemsicherheit nicht gewährleistet, erhöht sich die Gefahr von Betrugs- oder Diebstahlsdelikten. Auch bei der Sorge um den Schutz der Sicherheit gilt: je grösser die Sicherheitsbedenken und je höher somit die Risikowahrnehmung, desto kleiner die Wahrscheinlichkeit des Zustandekommens einer Online-Transaktion. Umgekehrt gilt: Vertrauen reduziert die Sorgen hinsichtlich der Sicherheitsrisiken – eine mögliche Transaktion wird dadurch erleichtert (Urban et al. 2009).

Die Sorge der Bürger um ihre Privatsphäre und die Datensicherheit prägt die Rezeption des nPA maßgeblich. Nachrichten in den globalen Medien über Sicherheitslecks, Internetkriminalität und ‚Phishing'-Angriffe steigern die Sensibilität der Menschen zusätzlich und erschweren die Akzeptanz digitaler Ausweis-Projekte. Nach Petkovic und Jonker ist es darum bei der Einführung neuer Technologien stets sehr wichtig, den Schutz der Privatsphäre und die Sicherheit sicherzustellen (Petkovic/Jonker 1998, 1).

Um die Privatsphäre sicherzustellen, sollten Regierungen Regeln aufstellen und diese den Bürgern sowie den Angestellten vermitteln. Solche Regeln für E-Government-Projekte wurden etwa in Großbritannien beispielhaft definiert. Datenschutzbeauftragte haben hier acht Datenschutzrichtlinien einzuhalten. Diese schreiben vor, dass persönliche Daten (UK Cabinet Office 2002, 31):

(1) ordentlich und rechtmäßig bearbeitet werden,
(2) für bestimmte und rechtmäßige Zwecke erhalten und bearbeitet werden,
(3) angemessen, relevant und nicht unverhältnismäßig sind,
(4) fehlerfrei und aktuell sind,
(5) für nicht länger als nötig aufbewahrt werden,
(6) in Übereinstimmung mit den Rechten des Bürgers bearbeitet werden,
(7) sicher aufbewahrt werden,
(8) innerhalb der EU bleiben, außer es gibt ausreichende Sicherheitsmaßnahmen.

Falls persönliche Daten im Namen eines Datenschutzbeauftragten von einer dritten Person weiterverarbeitet werden, müssen die Aktivitäten der datenverarbeitenden Instanz durch einen schriftlichen Vertrag geregelt werden. Zusätzlich müssen Dienstleister, die Registrierungsdienste für die öffentliche Verwaltung anbieten, jede Vorgabe bezüglich des Datenschutzes und der Speicherung erfüllen. Einige konkrete Punkte, die in Bezug auf den Zugang zu E-Government-Diensten entstehen, werden im Folgenden dargestellt (UK Cabinet Office 2002, 31ff):

a) Durch Einhaltung der siebten Richtlinie muss die Authentifizierung und Registrierung unbefugte Auskunft über persönliche Daten verhindern: Tatsächlich wird es mit großer Wahrscheinlichkeit so sein, dass der Mechanismus für die Freigabe von Daten für einen bestimmten Behördendienst stärker sein wird, als für die Vorlage der Daten im ersten Schritt.
b) Daten, die zur Überprüfung einer realen Identität erhalten wurden, sollten nicht für sekundäre Zwecke genutzt werden.
c) Es muss Transparenz herrschen: Es sollte für den Dateninhaber ersichtlich sein, warum Anmelde- oder Registrierungsinformationen benötigt werden.
d) Obwohl es während der Überprüfung der realen Identität nötig sein kann, Informationen für einen überschaubaren Zeitraum zu speichern, z.B. aus Gründen der Zurechenbarkeit und der Kontrolle, müssen die Anforderungen der fünften Richtlinie beachtet werden.

e) Wo ein Trust-Service-Provider einen Kunden im Auftrag einer oder mehrerer vertrauenswürdiger Institutionen (wie in diesem Fall eine “Portal-Dienstleistung") registriert, darf der Trust-Service-Provider nur Informationen die relevant sind an vertrauenswürdige Institutionen weitergeben.

Zusammenfassend können das Vertrauen der Nutzer und ihre Risikowahrnehmung als zentrale personenbezogene Einflussfaktoren der Akzeptanz neuer elektronischer Angebote betrachtet werden. Vertrauen ist immer dann besonders wichtig, wenn soziale Situationen durch Risiko, Unsicherheit und gegenseitige Abhängigkeit gekennzeichnet sind (McKnight/Chervany 2002). Vertrauen kann eine Risikowahrnehmung dabei nicht beseitigen, doch es hilft, diese zu reduzieren. Obwohl gewisse individuelle Eigenschaften – wie die Persönlichkeit und vergangene Erfahrungen – eine Rolle bei der Bestimmung des wahrgenommenen Risikos und der Höhe des Vertrauens spielen, können diese Faktoren durch gezielte Kommunikation und transparente Sicherheitsmaßnahmen gefördert werden.

2.2.2.3. *Beispiele personenbezogener Faktoren*

Heute übliche Identifikationsmethoden

Im täglichen Leben erfolgt die Identifikation mithilfe von Ausweisen. In Online-Umgebungen war es bisher jedoch nicht möglich, einen Personalausweis vorzuzeigen. Mehrere Online-Transaktionen (insbesondere Online-Banking und E-Commerce) wären sicherer, wenn elektronische Ausweise benutz werden würden. Aufgrund des Fehlens von technischen Möglichkeiten der Online-Identifikation, werden daher kompliziertere und langwierige Prozesse verwendet. Die am häufigsten in Deutschland verwendeten sind:

- **Postident-Verfahren:** Das ‚Postident-Verfahren‘ der Post AG, das nur mit Medienbrüchen möglich ist, erfordert eine Reihe aufwendiger Schritte und bringt zusätzliche Kosten mit sich (Deutsche Post, 1). Es wird gewöhnlich für die Eröffnung eines Bankkontos oder den Verkauf von Produkten an Kinder oder junge Erwachsene verwendet, um das Jugendschutzgesetz einzuhalten (Bundesministerium für Familie 2009).
- **PIN-TAN-Verfahren:** Das PIN-TAN-Verfahren, stellt ein Sicherheitsverfahren dar, das vorwiegend im Online-Banking eingesetzt wird. Das System beruht auf der Verwendung der persönlichen Identifikationsnummer (PIN) und Transaktionsnummern (TAN). Während also die PIN eine Person eindeutig identifiziert, legitimiert die TAN die Durchführung einer bestimmten Handlung (Transaktion). Die Gültigkeit der TAN ist auf deren einmalige Verwendung beschränkt, die PIN hingegen behält ihre Gültigkeit bis zur Änderung durch den Nutzer. Konkret sieht das Verfahren so aus, dass eine Person zunächst eine PIN erhält und eine Liste mit zufälligen TANs, die auf getrenntem und sicherem Wege postalisch zugestellt wird. Zur Durchführung einer Transaktion wird der Nutzer zunächst gebeten, seine PIN einzugeben. Anschlie-

ßend muss die geforderte TAN auf der TAN-Liste gesucht und eingegeben werden. Das PIN-TAN-Verfahren gilt gegenüber kryptografischen Authentifizierungsverfahren als veraltet und umständlich. Da aber auf der Client-Seite keine zusätzlichen technischen Hilfsmittel wie z. B. Kartenleser oder Ähnliches benötigt werden, ist das PIN-TAN-Verfahren universell einsetzbar und erfreut sich daher immer noch großer Beliebtheit.

Risikowahrnehmung im Falle des nPA

Um vertrauensfördernde Faktoren im Rahmen der Einführung neuer Identifikations- und Authentifizierungsverfahren zu identifizieren, ist es wichtig die grundlegenden Bedenken der Bürger in Bezug auf das Projekt zu verstehen. Eine umfangreiche Literaturanalyse und eine Internetrecherche zeigen, dass es hinsichtlich des nPA verschiedene Bedenken der Nutzer gibt. Eine ausführliche Auflistung der Bedenken befindet sich im Anhang, die wichtigsten Faktoren sind:

(1) **Was passiert bei Verlust des Ausweises?** Die Gefahr des Verlustes oder des Diebstahls der Karte gefährdet persönliche Daten.
(2) **Die Regierung versucht alle persönlichen Daten aufzuzeichnen:** Es besteht das Risiko des ‚gläsernen Bürgers‘.
(3) **Dritte können auf Daten inklusive der Biometrie mithilfe von RFID zugreifen:** Es existiert die Gefahr des nicht autorisierten Zugriffs eines Dritten auf persönliche und biometrische Daten.
(4) **Es ist sehr teuer:** Es entstehen höhere Kosten für den digitalen Ausweis und es werden bestimmte Bestandteile, wie die AusweisApp und ein berührungsloses Kartenlesegerät, notwendig.

Eine Umfrage von TNS Infratest (o. V. 2010a), bei der 1002 deutsche Onliner ab 18 Jahren befragt wurden, ergab, dass Sicherheit bei E-Government-Angeboten für die Befragten an vorderster Stelle steht. Insgesamt sind Datenschutz und Datensicherheit, Sicherheit im Allgemeinen sowie die Zuverlässigkeit der Systeme für Onliner in Deutschland die wichtigsten Aspekte bei der Abwicklung von Behördengängen im Internet. Circa vier von fünf Umfrageteilnehmern sind diese Punkte sehr oder sogar äußerst wichtig, bei Personen die bereits E-Government-Angebote online genutzt haben, erhöht sich dieser Anteil sogar auf circa 90 % der Befragten. Weiter sind neben inhaltlichen Aspekten, wie Aktualität der Inhalte und Angebote, auch Vertrauen in die jeweilige Behörde und die einfache Bedienbarkeit besonders wichtige Anforderungen an E-Government-Angebote (o. V. 2010a, 13f). Abbildung 5 stellt die Relevanz verschiedener Aspekte bei der elektronischen Abwicklung von Behördengängen im Internet grafisch dar.

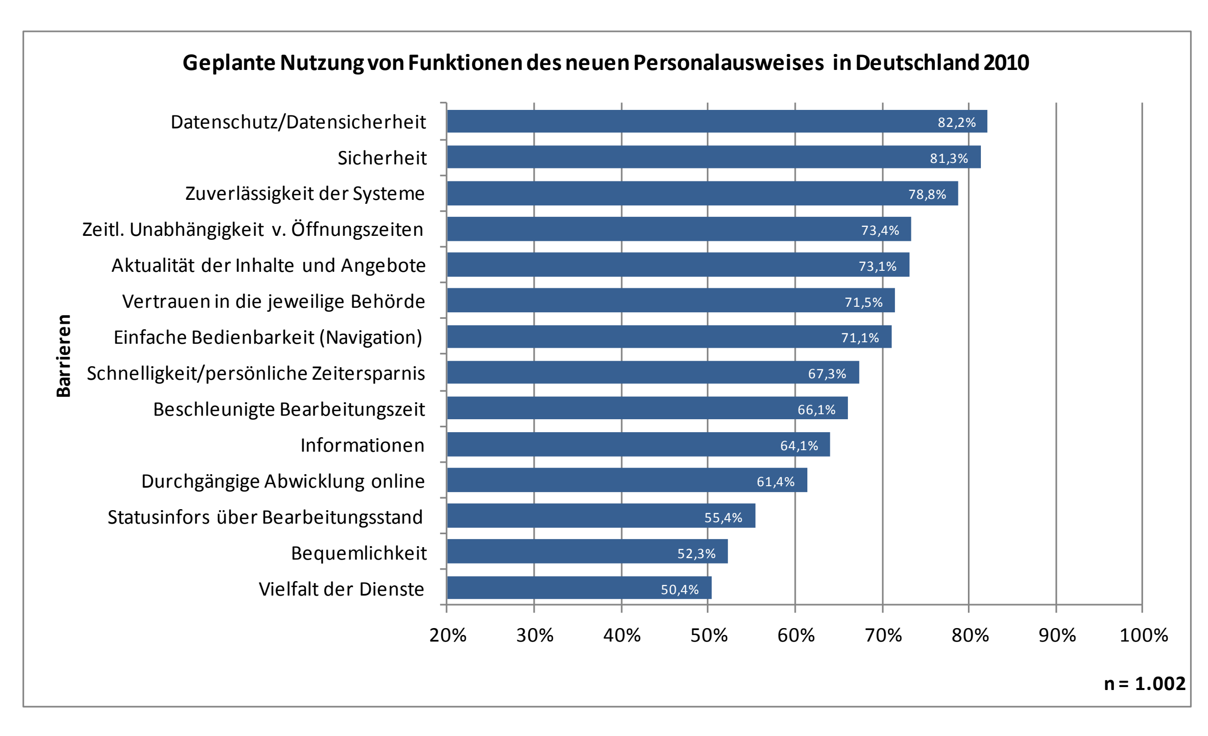


Abbildung 5: Wichtigkeit verschiedener Aspekte bei der elektronischen Abwicklung von Behördengängen im Internet (o. V. 2010a, 13)

Die größten Nutzungsbarrieren für E-Government-Angebote, die einer generellen oder intensiveren Nutzung der Online-Angebote vonseiten der Nutzer im Weg stehen, sind Punkte, die die Bedienbarkeit oder Usability der Angebote anbelangen. Eine mangelnde Durchgängigkeit, also Medienbrüche sowie undurchschaubare Strukturen der Online-Angebote, bilden die Gruppe der am häufigsten genannten Hemmnisse. Circa 33 % der Befragten sehen auch eine mangelnde Datensicherheit bzw. Datenschutz als Barriere. Ebenso nennen circa 26 % der Befragten mangelndes Vertrauen in die Behörde bzw. circa 24 % der Befragten die Unpersönlichkeit der Online-Abwicklung als Nutzungsbarrieren (o. V. 2010a, 13f). In Abbildung 6 werden die Nutzungsbarrieren der Befragten nochmals veranschaulicht.

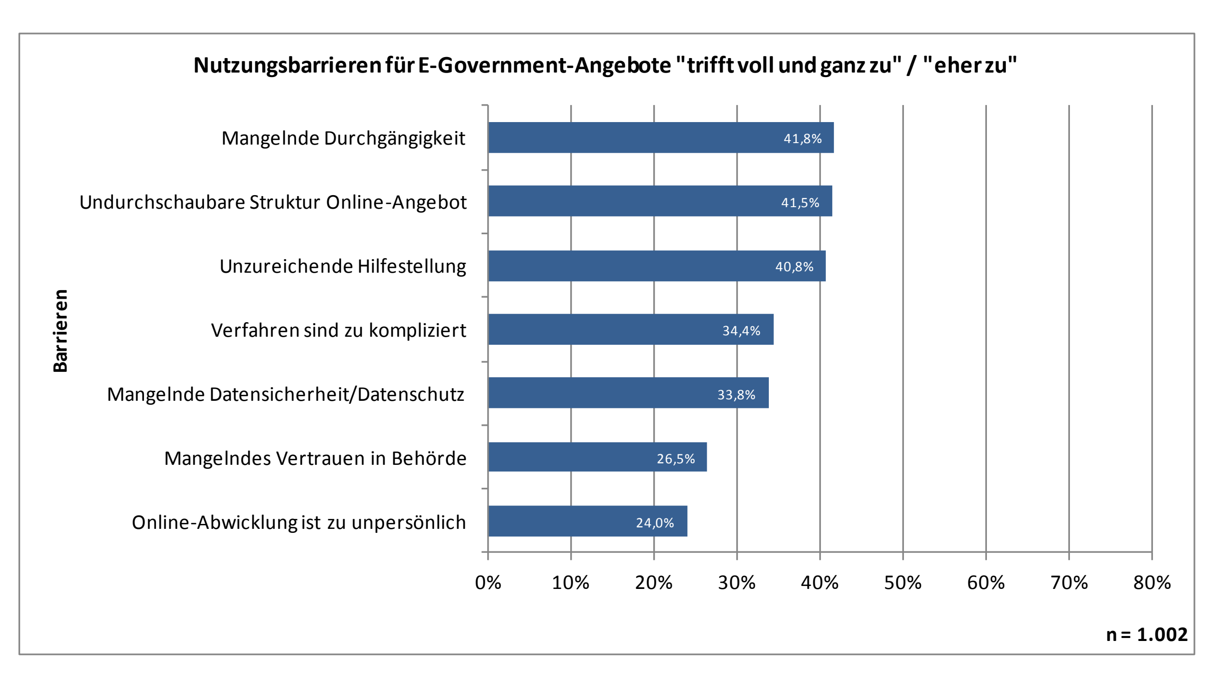


Abbildung 6: Nutzungsbarrieren für E-Government-Angebote (o. V. 2010a, 14)

In Abbildung 6 wurde zwar der mangelnde Datenschutz bereits angesprochen, in Abbildung 7 wird dieser Aspekt allerdings nochmals genauer beleuchtet. Demnach ist die Befürchtung, durch die Datenzusammenführung in einer zentralen Datenbank ein „gläserner Bürger“ zu werden, altersabhängig: Circa 65 % der Umfrageteilnehmer ab 35 Jahren, für die Datensicherheit/-schutz eine Nutzungsbarriere darstellt, haben diesbezüglich Bedenken. Bei der Altersgruppe zwischen 18 und 34 Jahren haben nur circa die Hälfte der Befragten Bedenken hinsichtlich des „gläsernen Bürgers“. Bei dieser Altersgruppe stehen hingegen Bedenken hinsichtlich der mangelnden Sicherheit bei der Übertragen stärker im Vordergrund (o. V. 2010a, 14).

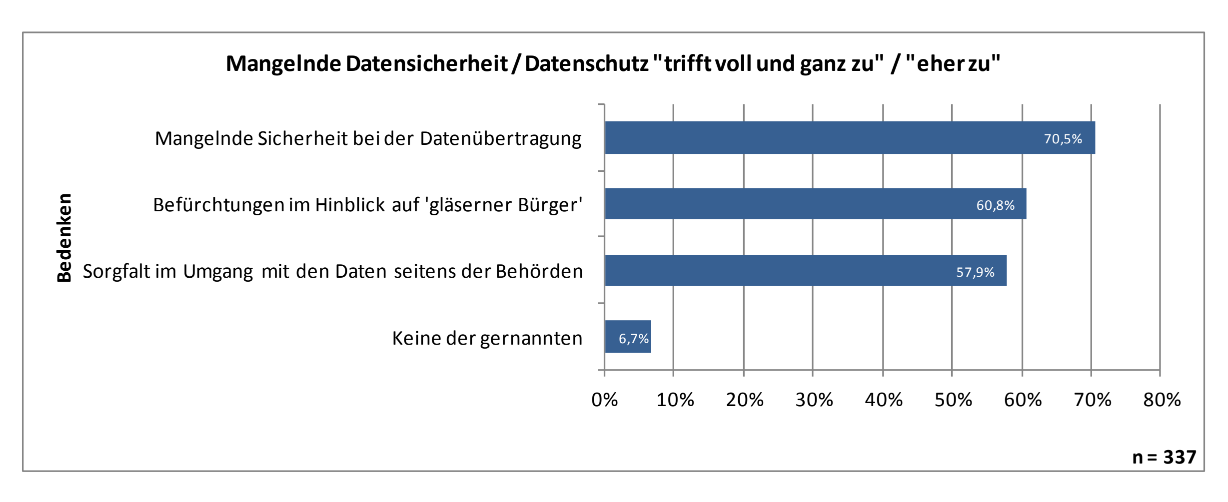


Abbildung 7: Bedenken speziell beim Datenschutz (o. V. 2010a, 14)

Die Frage nach der Akzeptanz von Sicherheitstechnologien durch den Nutzer wird weiterhin eine Schlüsselrolle bei der Absicherung zukünftiger Systeme bleiben. Nach wie vor werden Sicherheitstechnologien beim Endnutzer häufig aufgrund ihrer mangelnden Transparenz, schwierigen Bedienbarkeit und Kosten abgelehnt. Eine weitere Frage, die sich mit der Nutzung des nPA ergibt, ist die Frage nach der Verantwortung für die persönlichen Daten und die damit einhergehende Kontrollierbarkeit der weiteren Verbreitung der Daten, wenn diese im Internet preisgegeben worden sind.

Zusammenfassend kann festgehalten werden, dass Bürger für die Sicherheit der im Internet veröffentlichten und verarbeiteten Daten künftig eine sehr viel größere Verantwortung zu übernehmen haben. An dieser Stelle ist aber auch die Privatwirtschaft gefordert. Diese hat einfach zu nutzende, qualitativ hochwertige Sicherheitslösungen zu entwickeln, die Bürgern ermöglichen, den Zugriff auf die persönlichen Daten im Internet, deren Verarbeitung und Löschung durchgängig zu kontrollieren. Auf der anderen Seite ist der Staat gefordert, angemessene Aufklärungsarbeit zu leisten, um Bürger über Gefahren, Rechte und Pflichten im Umgang mit ihren persönlichen Daten aufzuklären. Außerdem werden rechtliche Vorgaben erforderlich, sodass Hersteller und Anbieter von Produkten bzw. Online-Dienstleistungen verpflichtet sind, hohe technische Qualitätsstandards für ihre Produkte nachzuweisen (o. V. 2010c, 100ff).

Adressierung möglicher Risiken

Durch die Nutzung des nPA können Schäden, die durch elektronische Diebstähle entstehen, vermieden werden. Aus diesem Grund ist es für die Erhöhung des Vertrauens in den nPA wichtig, mögliche Risiken von Online-Transaktionen (Phishing, Skimming, Computer Hacking) zu adressieren:

- **Phishing** – abgeleitet von “fishing” – ist der betrügerische Versuch, üblicherweise über E-Mails, persönliche Informationen wie Kreditkartennummer, Kontonummer oder Passwörter zu stehlen. Bei einem Phishing-Angriff erhält der Nutzer eine E-Mail, die den Anschein erweckt, von einem seriösen Absender, wie z. B. PayPal, zu kommen. In der E-Mail ist angegeben, dass persönliche Informationen aktualisiert oder bestätigt werden müssen. Nachdem man dem Link, der in der E-Mail angegeben ist, auf die Webseite gefolgt ist und anschließend die persönlichen Informationen angegeben hat, ist das Phishing abgeschlossen.
- **Skimming** ist das illegale Erfassen bzw. Kopieren einer rechtmäßigen Kreditkarte und die anschließende Erstellung einer gefälschten Kreditkarte mithilfe elektronischer Mittel (Commonwealth of Australia 2006, 1).
- **Computer Hacking:** Dabei wird mithilfe von Assemblersprachen oder einer Sprache auf Systemebene in ein Computersystem eingedrungen.

Phishing ist die größte Bedrohung, die bei der Nutzung digitaler Ausweise entstehen kann. Die Techniken, die von ‚Phishern‘ genutzt werden, sind ausgeklügelt, was es für unerfahrene Nutzer schwer macht, ‚Phishing‘ zu erkennen. Aufgrund der steigenden Zahl von Online-Firmen und -Transaktionen ist ein Anstieg solcher Attacken zu erwarten.

Wenn Bürger neue Personalausweise bei E-Business- und E-Government-Anwendungen einsetzen würden, wäre die Zahl der Phishing Angriffe viel geringer. Deshalb sollten die Kommunikationsmaßnahmen der Regierung auch gegenwärtige Risiken beinhalten und aufzeigen, wie diese durch den Einsatz von neuen Personalausweisen verringert werden können. In Deutschland gibt es zurzeit eine Webkampagne mit Filmen, Flyern und einem detaillierten Webportal (https://www.sicher-im-netz.de/Default.aspx), das sich mit der Schaffung von Sicherheit bei Online-Transaktionen beschäftigt.

Weitere Sicherheitsmassnahmen: De-Mail und De-Safe

Der neue Personalausweis befähigt Bürger, rechtlich bindende Online-Transaktionen mit der Regierung und anderen Partnern durchzuführen. Der nPA ermöglicht die elektronische Authentifizierung. Falls es der Kartenbesitzer wünscht, kann eine qualifizierte elektronische Signatur zum nPA hinzugefügt werden. Dies erleichtert rechtliche Transaktionen, die normalerweise eine handgeschriebene Unterschrift benötigen. Um die Kommunikation über das Internet weiter abzusichern, wird mittels De-Mail und De-Safe die Sicherheit des gängigsten Kommunikationsmittels (E-Mail) gewährleistet (o. V. 2011a). Mittels De-Mail können Dokumente und Nachrichten verbindlich und vertraulich versendet

werden, ohne dass der Absender oder Empfänger weitere Software oder Hardware installieren muss. Bürger können dafür abgesicherte Webanwendungen von De-Mail-Providern verwenden (Bundesministerium des Inneren 2011). Für einen erfolgreichen Versand werden alle Kommunikationspartner authentifiziert, die Nachricht über eine abgesicherte Verbindung zum Provider geschickt und die Transportwege der Nachricht verschlüsselt, sodass ihr Inhalt nicht mitgelesen oder verändert werden kann. Die Anbieter von De-Mail werden vom Bundesamt für Sicherheit in der Informationstechnik geprüft. Erst wenn sie akkreditiert werden, können sie am Markt auftreten. Durch die Akkreditierung von Anbietern, die Authentifizierung von Kommunikationspartnern und die Verschlüsselungsverfahren wird ein abgesichertes Versenden und Empfangen von Nachrichten und Dokumenten ermöglicht. Die Verwendung von De-Mail erlaubt geschäftliche oder behördliche Kommunikation, die rechtlich verbindlich ist und vollständig elektronisch erfolgt (Bundesministerium des Inneren 2011). Die Speicherung sensibler oder auch vertraulicher Daten erfolgt nicht auf Rechnern, da es dort kaum möglich ist, Daten absolut geschützt aufzubewahren. Mit der Funktion „De-Safe“ können Nutzer ihre sensiblen elektronischen Dokumente sicher archivieren. Die Daten werden verschlüsselt gespeichert und vor Verlust und Manipulation geschützt (o. V. 2011a). Erst nach einer erfolgreichen Authentifizierung des Nutzers kann auf die Daten zugegriffen werden. Das Authentifizierungsniveau wird vom Nutzer vorbestimmt und variiert von einem normalen – Verwendung eines Passwort – bis zu einem sehr hohen Sicherheitsniveau – zum Beispiel Authentifizierung mittels nPA (o. V. 2011a). Insgesamt wird durch De-Mail und De-Safe eine Infrastruktur zur sicheren und verbindlichen elektronischen Kommunikation geschaffen. Maßgeblich für den Erfolg dieser Infrastruktur ist ihre Vertrauenswürdigkeit. Die Sicherheitsanforderungen des De-Mail Gesetzes (De-Mail-Gesetz, BT-Drs. 17/3630) und das Akkreditieren der Providern stellen sicher, dass die sensiblen Daten und die Privatsphäre der Bürger geschützt werden.

2.2.3. Vertrauensstufen bei E-Government-Dienstleistungen

Basierend auf einer Literaturrecherche konnten Kriterien, wie Vertrauen, Sicherheit, Privatsphäre und Authentifizierungsmethoden bei der Gestaltung und Nutzung der AusweisApp und des nPA als bedeutsam für deren Adoption identifiziert werden. Weiter wurde dargestellt, wie Vertrauen für die Nutzung des nPA gefördert werden kann und welche technischen und sozialen Voraussetzungen für Vertrauen existieren. Ein Ansatz, Vertrauen zu fördern, besteht im Einsatz von Applikation wie De-Mail und dem zugehörigen De-Safe. Der folgende Abschnitt differenziert darauf aufbauend, welche und wie viele Vertrauensstufen für E-Government- und E-Business-Anwendungen notwendig sind. Die Wahl der Vertrauensstufe hängt vom wahrgenommenen Risiko der Bürger ab, welches je nach Bürger variiert.

Wie bereits erwähnt, geht Vertrauen mit dem wahrgenommenen Risiko einher (Kim et al. 2008, 544). Deshalb ist die Stufe des Vertrauens, die für eine Transaktion nötig ist, auch vom jeweiligen Transak-

tionsrisiko abhängig. Aus diesem Grund werden verschiedene Vertrauensstufen für unterschiedliche Transaktionen benötigt. Das wahrgenommene Risiko unterscheidet sich von Person zu Person. Es ist nicht einfach, Vertrauensstufen für verschiedene Anwendungen mit digitalen Ausweisen festzulegen. Empirische Studien über die Wahrnehmung des Risikos einer speziellen Anwendung können analysiert und Vertrauensstufen durch die Einbeziehung einer durchschnittlichen Risikowahrnehmung der Bürger bestimmt werden.

In der Literatur werden drei Vertrauensstufen (von grundlegend bis erweitert) definiert:

(1) **Grundlegende Vertrauensstufe:** Die grundlegende Vertrauensstufe wird für die Teilnahme an einer Online-Transaktion benötigt, z. B. Log-in mit Benutzernamen und Passwort
(2) **Geschützte Vertrauensstufe:** z. B. bei Nutzung einer Kreditkarte für E-Commerce-Anwendungen
(3) **Erweiterte Vertrauensstufe:** Dies ist die restriktivste Vertrauensstufe, z. B. online Speicherung der Kreditkarteninformationen für die zukünftige Nutzung von E-Commerce-Anwendungen

Beispiel USA

Für E-Government Anwendungen wurden bisher unterschiedliche Vertrauensstufen in verschiedenen Projekten genutzt. In den USA wurden vier Sicherheitsstufen für E-Government Transaktionen definiert (Executive Office of the President 2003, 4f):

- **Stufe 1 (wenig oder kein Vertrauen in die Validität der angegebenen Identität):** Bei dieser Stufe existiert wenig oder kein Vertrauen in die angegebene Identität. Zum Beispiel erlauben Berechtigungsnachweise der Stufe 1 das Setzen von Lesezeichen auf Elemente/Artikel einer Webseite für die künftige Verwendung.
- **Stufe 2 (etwas Vertrauen in die Validität der angegebenen Identität):** Berechtigungsnachweise der Stufe 2 eignen sich für ein breites Spektrum von Angelegenheiten im Austausch mit der Öffentlichkeit, bei denen Behörden anfängliche Identitätsangabe benötigen. Hierbei werden die Details vor jedem staatlichen Handeln einzeln überprüft.
- **Stufe 3 (hohes Vertrauen in die Validität der angegebenen Identität):** Stufe 3 ist adäquat für Transaktionen, die hohes Vertrauen in die Validität der angegebenen Identität benötigen. Nutzer mit Berechtigungsnachweisen der Stufe 3 haben ohne weitere Identitätskontrollen Zugang zu eingeschränkten Web Dienstleistungen.
- **Stufe 4 (sehr hohes Vertrauen in die Validität der angegebenen Identität):** Stufe 4 ist adäquat für Transaktionen, die sehr hohes Vertrauen in die Validität der angegebenen Identität benötigen. Nutzer legen Berichtigungsnachweise der Stufe 4 zur Bestätigung ihrer Identität

vor, und erhalten ohne eine weitere Identitätskontrolle Zugang zu hoch beschränkten Webquellen.

Die benötigten Sicherheitsstufen für elektronische Transaktionen wurden durch eine Bewertung der Risiken für jede Transaktion festgelegt. Realisiert wurde dies durch die Analyse sowohl der Risiken als auch deren Eintrittswahrscheinlichkeit. Ein Ziel war auch die Ermittlung von Maßnahmen zur Minimierung der Auswirkungen potentieller Risiken im Falle eines Authentifizierungsfehlers. Alle Risiken der folgenden Kategorien wurden analysiert:

- Belästigung, Notlage oder Schädigung von Ansehen oder Ruf,
- Finanzieller Verlust oder Haftung einer Behörde,
- Schaden für Behördenprogramme oder am öffentlichen Interesse,
- Nicht genehmigte Veröffentlichung von sensiblen Informationen,
- Persönliche Sicherheit,
- Zivile oder kriminelle Verstöße.

Die Analyse basiert auf den potenziellen Auswirkungen der Risiken, die in drei Kategorien (niedrig, mittel und hoch) eingeteilt wurden:

	Niedrig	Mittel	Hoch
Belästigung, Notlage oder Schaden für Ansehen oder Ruf	Im schlimmsten Fall entsteht eine eingeschränkte, kurzfristige Belästigung, Notlage oder Schädigung von Ansehen oder Ruf irgendeiner Partei	Im schlimmsten Fall entsteht eine ernsthafte kurzfristige oder eingeschränkte langfristige Belästigung, Notlage oder Schädigung von Ansehen oder Ruf irgendeiner Partei	Es entsteht eine heftige oder ernsthafte langfristige Belästigung, Notlage, oder Schädigung von Ansehen oder Ruf irgendeiner Partei (üblicherweise ist diese Kategorie für Situation mit besonders schweren Auswirkungen oder für solche, die viele Individuen betreffen, vorbehalten)
Finanzieller Verlust oder Haftung einer Behörde	Im schlimmsten Fall entsteht ein unbedeutender bzw. irrelevanter und nicht behebbarer finanzieller Verlust für irgendeine Partei oder schlimmstenfalls eine unbedeutende bzw. irrelevante Haftung von einer Behörde	Im schlimmsten Fall entsteht ein ernsthafter und nicht behebbarer finanzieller Verlust für irgendeine Partei oder eine gravierende Haftung von einer Behörde	Es entsteht ein heftiger oder katastrophaler und nicht behebbarer finanzieller Verlust für irgendeine Partei oder eine sehr hohe bzw. katastrophale Haftung von einer Behörde
Schaden für Behördenprogramme oder für das öffentliche Interesse	Im schlimmsten Fall entsteht ein beschränkter und nachteiliger Einfluss auf die betriebliche Tätigkeit, das Vermögen der Organisation oder das öffentliche Interesse. Beispiele für beschränkte nachteilige Einflüsse sind:	Im schlimmsten Fall entsteht ein ernsthafter nachteiliger Einfluss auf die betriebliche Tätigkeit, Vermögen der Organisation oder das öffentliche Interesse. Beispiele für ernsthafte nachtei-	Es entsteht ein heftiger und katastrophaler Einfluss auf die betriebliche Tätigkeit, das Vermögen der Organisation oder das öffentliche Interesse. Beispiele für heftige und katastrophale Einflüsse sind: (i) massiver Abbau der Einsatzfähigkeit soweit und

	Niedrig	Mittel	Hoch
	(i) Abbau der Einsatzfähigkeit soweit und so lange, dass die Organisation noch fähig ist seine primären Funktionen ohne merklich reduzierte Effektivität auszuführen (ii) geringfügiger Schaden am Vermögen der Organisation oder am öffentlichen Interesse	lige Einflüsse sind: (i) signifikanter Abbau der Einsatzfähigkeit soweit und solange, dass die Organisation fähig ist, seine primären Funktionen mit signifikant reduzierter Effektivität auszuführen (ii) signifikanter Schaden am Vermögen der Organisation oder am öffentlichen Interesse	solange, dass die Organisation nicht mehr fähig ist, eine oder mehrere ihrer primären Funktionen auszuführen (ii) bedeutender Schaden am Vermögen der Organisation oder am öffentlichen Interesse
Nicht genehmigte Veröffentlichung von sensiblen Informationen	Im schlimmsten Fall kommt es zu einer eingeschränkten Veröffentlichung von persönlichen, U.S. regierungssensiblen oder kommerziell sensiblen Informationen an nicht autorisierte Parteien, was zu einem Vertrauensverlust mit geringer Auswirkung führt	Im schlimmsten Fall kommt es zu einer Veröffentlichung von persönlichen, U.S. regierungssensiblen oder kommerziell sensiblen Informationen an nicht autorisierte Parteien, was zu einem Vertrauensverlust mit mittlerer Auswirkung führt	Es kommt zu einer Veröffentlichung von persönlichen, U.S. regierungssensiblen oder kommerziell sensiblen Informationen an nicht autorisierte Parteien, was zu einem Vertrauensverlust mit hoher Auswirkung führt
Persönliche Sicherheit	Im schlimmsten Fall kommt es zu geringen Verletzungen, die keine medizinische Behandlung erfordern	Im schlimmsten Fall besteht das mittlere Risiko von geringen Verletzungen oder das geringe Risiko von Verletzungen, die medizinische Behandlung erfordern	Es entsteht das Risiko von ernsthaften Verletzungen oder dem Tod
Zivile oder kriminelle Verstöße	Im schlimmsten Fall entsteht das Risiko von zivilen oder kriminellen Verstößen, die normalerweise nicht Grundlage für Vollstreckungsbemühungen sind	Im schlimmsten Fall entsteht das Risiko von zivilen oder kriminellen Verstößen, die Grundlage für Vollstreckungsbemühungen sein können	Es entsteht das Risiko von zivilen oder kriminellen Verstößen, die von besonderer Bedeutung für Vollstreckungsmaßnahmen sind

Tabelle 3: Potentielle Auswirkungen von Authentifizierungsfehlern für E-Governmen-Dienste in den USA (Executive Office of the President 2003, 6ff.)

Anschließend wurden die nötigen Vertrauensstufen mithilfe von Tabelle 3 festgelegt. Die Zeilen repräsentieren die potenziellen Auswirkungskategorien des Authentifizierungsfehlers und die Spalten geben die nötige Vertrauensstufe an (vgl. Tabelle 4).

	1	2	3	4
Belästigung, Notlage, oder Schaden für Ansehen oder Ruf	Niedrig	Mittel	Mittel	Hoch
Finanzieller Verlust oder Haftung einer Behörde	Niedrig	Mittel	Mittel	Hoch
Schaden für Behördenprogramme oder öffentliches Interessen	N/A	Niedrig	Mittel	Hoch
Nicht genehmigte Veröffentlichung von sensiblen Informationen	N/A	Niedrig	Mittel	Hoch
Persönliche Sicherheit	N/A	N/A	Niedrig	Mittel Hoch
Zivile oder kriminelle Verstöße	N/A	Niedrig	Mittel	Hoch

Tabelle 4: Benötigte Vertrauensstufen für E-Government-Dienste in den USA (Executive Office of the President 2003)

In manchen Fällen kann sich die vorgeschlagene Stufe auf mehrere Vertrauensstufen beziehen. So entspricht bspw. ein mittlerer finanzieller Verlust der Vertrauensstufe 2 und 3. In solch einem Fall wird geraten, die Umstände genauer zu betrachten, um die passende Vertrauensstufe festzulegen.

Wie können also E-Government-Dienstleistungen hinsichtlich unterschiedlicher Vertrauensstufen dargestellt werden?

- Stufe 1: Ein Nutzer nimmt an einer Online-Diskussion auf der whitehouse.gov Webseite teil und muss hierfür außer Namen und Ort keine identifizierenden Informationen preisgeben. Falls angenommen wird, dass sich das Forum nicht mit sensiblen oder privaten Informationen beschäftigt, gibt es kein offensichtliches, anhaftendes Risiko.
- Stufe 2: Ein Berechtigter ändert über die Webseite der Sozialversicherung seinen eingetragenen Wohnsitz. Die Seite benötigt eine Authentifizierung, um sicherzustellen, dass die Adresse durch die berechtigte Person geändert wird. Diese Transaktion birgt ein geringes Belästigungsrisiko. Da behördliche Mitteilungen, die unter anderem Zahlungsbetrag, Kontostatus und Änderungsaufzeichnungen beinhalten, an den eingetragenen Wohnsitz des Berechtigten gesandt werden, existiert ein mittleres Risiko der nicht autorisierten Veröffentlichung von sensiblen persönlichen Daten. Die Regierung beschließt, dass das Risiko der nicht autorisierten Veröffentlichung einer Authentifizierung der Sicherheitsstufe 2 zugeordnet werden kann.
- Stufe 3: Ein Patentanwalt reicht elektronisch vertrauliche Patentinformation beim US Patent- und Markenamt ein. Eine unzulässige Offenlegung würde Wettbewerbern einen Wettbewerbsvorteil verschaffen.
- Stufe 4: Ein Vollzugsbeamter greift auf eine Datenbank zu, die Vorstrafen speichert. Unbefugter Zugriff könnte den Datenschutz und/oder Ermittlungen gefährden.

Beispiel Großbritannien

Ähnliche Vertrauensstufen wurden auch für E-Government-Dienstleistungen in Großbritannien definiert (UK Cabinet Office 2002, 16ff.):

Stufe	Potenzielle Auswirkungen	Beispiele
0 (minimaler Schaden)	Minimale Belästigung für irgendeine Partei; oder kein Risiko für die persönliche Sicherheit irgendeiner Partei; oder keine Veröffentlichung von persönlichen oder geschäftlich sensiblen Daten an Dritte; oder minimaler finanzieller Verlust für irgendeine Partei; oder keine Schädigung von Ansehen oder Ruf irgendeiner Partei; oder keine Notlage für irgendeine Partei; oder keine Unterstützung bei der Durchführung oder Behinderung bei der Aufklärung eines schweren Verbrechens	Ein Kunde liest oder lädt öffentlich verfügbare Informationen von einer Regierungswebseite herunter. Der Zugang zu diesen Informationen verlangt vom Kunden nicht die Offenlegung seiner realen Identität
1 (geringer Schaden)	Geringe Belästigung für irgendeine Partei; oder kein Risiko für die persönliche Sicherheit irgendeiner Partei; oder keine Veröffentlichung von persönlichen oder geschäftlich sensiblen Daten an Dritte; oder geringer finanzieller Verlust für irgendeine Partei; oder keine Schädigung von Ansehen oder Ruf irgendeiner Partei; oder geringe Notlage irgendeine Partei; oder keine Unterstützung bei der Durchführung oder Behinderung bei der Aufklärung eines schweren Verbrechens	Ein Kunde vereinbart ein Treffen mit einem Regierungsbeamten über das Internet. Der Berechtigungsnachweis gibt grundlegende Garantien, wie die Echtheit der angegebenen Identität, falls die dafür nötigen Informationen sicher im Berechtigungsnachweis eingebunden sind oder in Erfahrung gebracht werden können
2 (bedeutender Schaden)	Bedeutende Belästigung für irgendeine Partei; oder kein Risiko für die persönliche Sicherheit irgendeiner Partei; oder Veröffentlichung von persönlichen oder geschäftlich sensiblen Daten an Dritte; oder bedeutender finanzieller Verlust für irgendeine Partei; oder bedeutende Schädigung von Ansehen oder Ruf irgendeiner Partei; oder bedeutende Notlage für irgendeine Partei; oder Unterstützung bei der Durchführung oder Behinderung bei der Aufklärung eines schweren Verbrechens	Ein Kunde registriert sich für die Kommunalsteuer anknüpfend an einen Wohnort wechseln. Da es Rechtsfolgen für die Nichtzahlung gibt, wird erhebliches Vertrauen in die reale Identität des Kunden benötigt
3 (erheblicher Schaden)	Erhebliche Belästigung für irgendeine Partei; oder Risiko für die persönliche Sicherheit irgendeiner Partei; oder die Veröffentlichung von persönlichen oder geschäftlich sensiblen Daten an Dritte; oder erheblicher finanzieller Verlust für irgendeine Partei; oder erhebliche Schädigung von Ansehen oder Ruf irgendeiner Partei; oder erhebliche Notlage für irgendeine Partei; oder Unterstützung bei der Durchführung oder Behinderung bei der Aufklärung eines schweren Verbrechens	Ein Kunde wünscht einen Führerschein online zu beantragen. Wieder sind die Registrierungsanforderungen streng, da dieser ein akzeptierter Identitätsnachweis ist

Tabelle 5: Benötigte Vertrauensstufen für E-Government-Dienstleistungen in Großbritannien (UK Cabinet Office 2002, 16ff.)

2.2.4. Übersicht: Nutzer- und Innovations-Charakteristika

Während deutsche Staatsbürger verpflichtet sind, den nPA zu besitzen, ist dessen weitere Nutzung jedoch vollkommen freiwillig, solange Verwaltungsprozesse nicht ausschließlich als E-Government-Dienstleistungen angeboten werden. Dabei ist zu beachten, dass in anderen Ländern (z. B. Großbritannien) keine eID-funktionsfähige Karte für den Zugang zu E-Government Diensten notwendig ist. Angaben des Bundesministeriums für Wirtschaft und Technologie (BMWi) zufolge, haben im Jahr 2008 33 % der Privatpersonen und 70 % der Unternehmen E-Government-Dienstleistungen genutzt (Bundesministerium für Wirtschaft und Technologie 2009, 83ff). Dies zeigt, dass E-Government einerseits für Unternehmen sehr attraktiv ist, andererseits jedoch E-Government bei den Bürgern bis 2008 noch nicht vollständig etabliert wurde. Durch die Einführung des nPA soll die Akzeptanz auf Seiten der Bürger wie auch der Unternehmen aufgrund erhöhter Sicherheit und Medienbruchfreiheit erhöht werden. Die bereits erwähnte empirische Untersuchung der Bürgermeinungen zum nPA gibt auch Auskunft über die Erwartungen an dessen Nutzung. Einerseits zeigen die Ergebnisse, welche Funktionen des nPA Bürger in Zukunft nutzen würden. Andererseits äußerten sich diese zu den gewünschten Anwendungsmöglichkeiten der eID-Funktion. Demnach wird die Verfügbarkeit und Zuverlässigkeit der gewünschten Funktionalitäten sowie auch das Angebot elektronischer Dienstleistungen durch Unternehmen die Nutzung des nPA bei elektronischen Dienstleistungen vorantreiben.

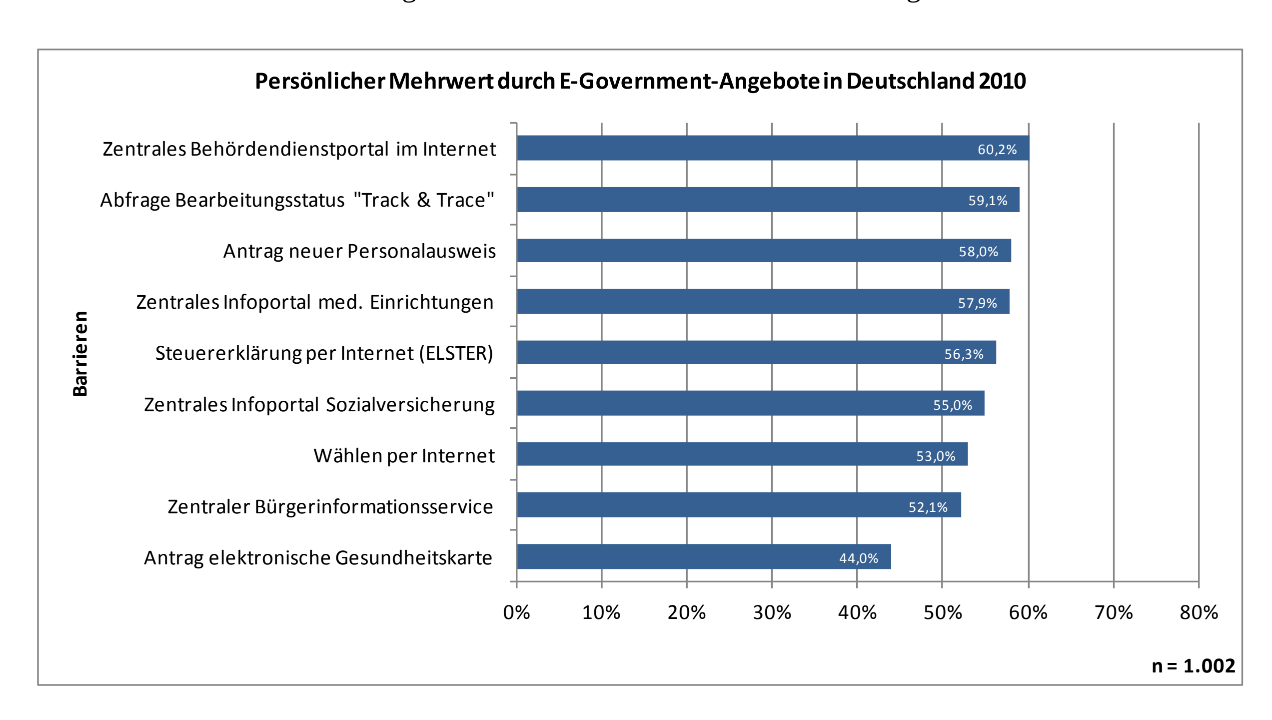


Abbildung 8: Persönlicher Mehrwert durch E-Government-Angebote in Deutschland 2010 (o. V. 2010a, 10)

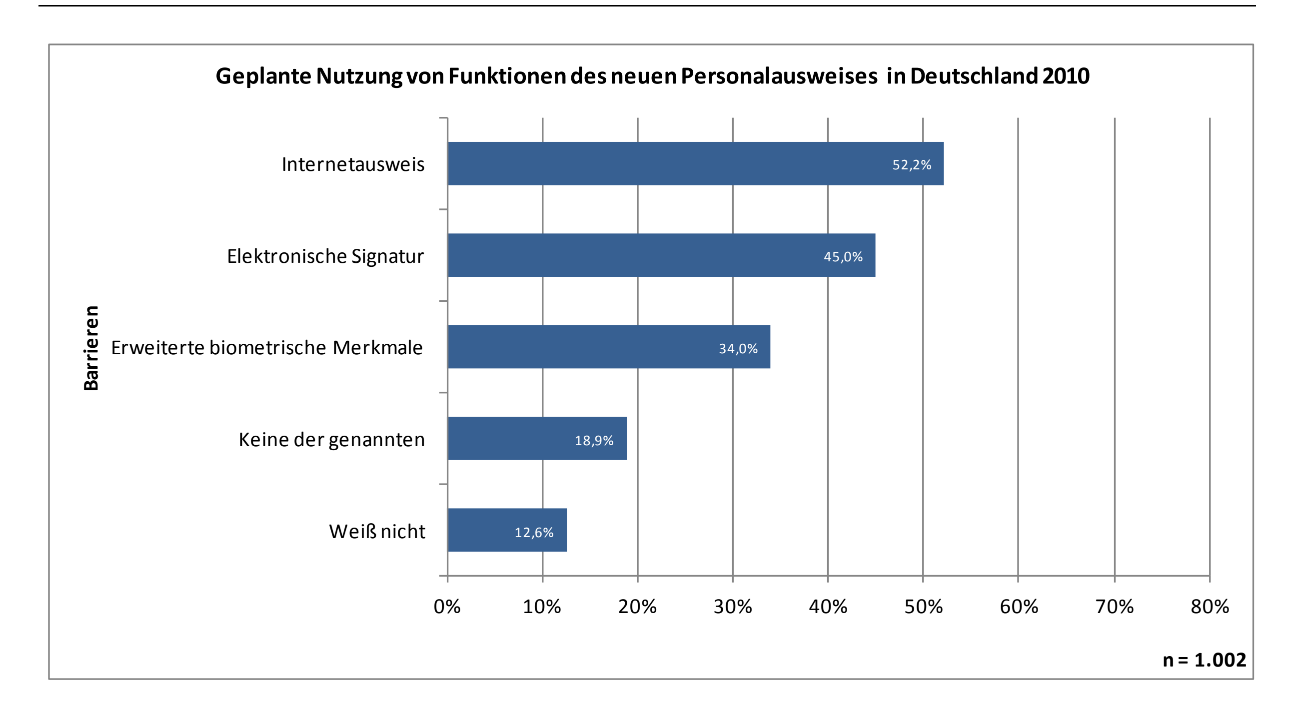


Abbildung 9: Geplante Nutzung von Funktionen des neuen Personalausweises in Deutschland 2010 (o. V. 2010a, 15)

Dies bestätigt die hier beschriebenen Theorien der Akzeptanz von IT-Innovationen. Innovationsbezogene Faktoren wie der relative Vorteil, die Kompatibilität oder Komplexität prägen die Abwägungen der Bürger – sei es in Form der wahrgenommenen Verfügbarkeit oder Zuverlässigkeit, sei es in Form eines breiten Angebots sinnvoller Funktionalitäten. Ebenso hatten wir gesehen, dass personenbezogene Einflussfaktoren, insbesondere Bedenken hinsichtlich des Datenschutzes und der Datensicherheit sowie Vertrauen einen massgeblichen Einfluss auf die Überlegungen der Bürger ausüben. Die hier beschriebenen Einflussfaktoren decken damit umfassende Aspekte innovativer Angebote ab – von dessen Kosten und Nutzen, technischen Eigenschaften, Design, Kommunikation und Vermarktung bis hin zum Vertrieb. Hinzu kommen Einflussfaktoren, welche durch Charakteristika des Angebots nicht unmittelbar beeinflusst werden können, wie das kulturelle und institutionelle Umfeld, verfügbare Infrastrukturen, Persönlichkeitseigenschaften sowie Einstellungen der Nutzer. Auch diese sind jedoch im Rahmen einer Einführungs- und Kommunikationsstrategie zu beachten.

Umfragen zeigen (vgl. Abbildung 9), dass 52,2 % der Bürger erwägen, die eID-Funktion und immerhin 45 % die qualifizierte elektronische Signatur zu nutzen. Dies wäre ein ermutigendes Signal hinsichtlich der Vermarktung des nPA und auch der Nutzung von elektronischen Dienstleistungen der Verwaltung. Es steht jedoch fest: die hier beschriebenen Zahlen hängen massgeblich von Eigenschaften des Angebots ebenso ab, sowie dessen Vermittlung an die Zielgruppen.

Zusammenfassung von Empfehlungen und Hinweisen bisher:

Zusammenfassend lässt sich festhalten, dass eine kontinuierliche Nutzung der Funktionen des nPA durch Bürger und Wirtschaftsakteure eine hohe Akzeptanz bedingt. Gesetzliche Vorschriften regeln die Adoptionsraten, indem die Entscheidung zur Übernahme des nPA nicht mehr den Bürgern überlassen ist. Allerdings lässt sich daraus allein nicht auf die langfristige Akzeptanz sowie die individuellen Nutzungsentscheidungen der Bürger schliessen. Massenmedien haben nur bedingt einen Einfluss auf die Akzeptanz einer Innovation, wie sie der nPA darstellt. Mittel- bis langfristig ausschlaggebend sind die hier beschriebenen innovations- und personenbezogenen Faktoren.

Aus der Betrachtung der innovations- und personenbezogenen Faktoren können diverse Erkenntnisse und Empfehlungen abgeleitet werden:
Der nPA schafft einen relativen Vorteil gegenüber bisherigen Angeboten, indem er den Aufwand bei Online-Transaktionen reduziert. Mehrmalige Anmeldungen im Internet werden durch einen einheitlichen Identitätsnachweis ersetzt. Allerdings darf diese Funktion keine zusätzlichen Sicherheitsrisiken mit sich bringen, um von Bürgern als vorteilhaft gesehen zu werden. Viele Bürger haben Bedenken bezüglich der Wahrung ihrer Privatsphäre und halten die Nutzung der elektronischen Authentifizierungsfunktion und der Biometrie für risikoreich. Die Schaffung von Vertrauen kann aber dieses wahrgenommene Risiko mindern. Hierfür haben die Transparenz und die Pseudonymfunktion große Bedeutung. Auch die Schaffung strikter Regeln, neuer Datenschutzbestimmungen und gesetzlicher Vorschriften wird dazu beitragen, dass Bürger den nPA als sicher wahrnehmen. Weiter ist es wichtig, Bürger, die bisher elektronische Dienstleistungen nicht genutzt haben, von deren Vorteilen zu überzeugen und so als Nutzer zu gewinnen. Die Akzeptanz kann auch durch eine größere Anzahl und Vielfalt der Anwendungen des nPA und der qualifizierten elektronischen Signatur gefördert werden. Eine breitere Dienstleistungspalette seitens Verwaltungen und der Wirtschaft wird einen größeren Anreiz bei Bürgern schaffen, Gebrauch von diesen zu machen.

Für Wirtschaftsakteure sind ebenfalls Sicherheit und Zuverlässigkeit der Funktionen des nPA entscheidend. Um sie als Dienstleistungsanbieter zu gewinnen, sollten Vorteile für Unternehmen betont werden. Strategische Wettbewerbsvorteile, wie zum Beispiel der Aufbau von Vertrauen und die Steigung der Sicherheit bei der Abfrage persönlicher Kundendaten, werden zu einem höheren Umsatz führen. Weiter führt das Angebot elektronischer Dienstleistungen zu Kosteneinsparungen bei Anbietern, wie Wirtschaftsakteuren oder Behörden. Der Einsatz des nPA entlastet von Routineaufgaben und spart Bearbeitungszeit und Ressourcen, ermöglicht aber auch eine Ausweitung des Dienstleistungsangebots. Bisher konnten Behörden elektronisch nur Informationen und wenige elektronische Dienstleistungen anbieten. Die Funktionen des nPA ermöglichen eine Ausbreitung des Serviceangebots.

Die Betrachtung der Kompatibilität lässt darauf schließen, dass der Aufbau der technischen Infrastruktur eine zentrale Bedeutung zur Nutzung des nPA hat, also die Versorgung der Bürger mit Lesegerä-

ten. Dies soll nicht nur vom Staat, sondern auch von Wirtschaftsakteuren gefördert werden, zum Beispiel durch Verkauf und kostenlose Verteilung von Lesegeräten durch Banken und Versicherungsunternehmen (Die Beauftragte der Bundesregierung für Informationstechnik 2010; Scheffel 2010). Die Entwicklung der technischen Infrastruktur ist eng mit der Komplexität der Nutzung verbunden. Der nPA und seine Anwendungen richten sich an keine spezielle Zielgruppe, sondern an alle Bürger, weshalb die Komplexität der Verfahren für Bürger minimiert werden soll. Da die Bürger unterschiedliche technische und soziale Fähigkeiten haben, soll die Software zur Nutzung des nPA (AusweisApp) möglichst einfach gestaltet werden. Einfache, verständliche Benutzerführungen und diverse Unterstützungsoptionen wie Supportfunktionen fördern die Erlernbarkeit. Weiter trägt die Transparenz der Authentifizierungsverfahren dazu bei, dass Bürger bei ihren ersten Erfahrungen mit dem nPA dessen Sicherheit als hoch wahrnehmen. Bürger sollen ohne Schwierigkeiten die Anwendungen selber testen und die Vorteile gegenüber den Nachteilen abwägen können. Durch zentrale Anwendungstests wurde bereits die Praxistauglichkeit verschiedener Anwendungen erprobt.

Individuelle Erfahrungen, allgemeine Informiertheit und Vielfalt von elektronischen Dienstleistungsangeboten sind ausschlaggebend für die Akzeptanz des nPA. Des Weiteren zeigen Studienergebnisse, dass Bürger mit E-Government-Nutzungserfahrung elektronische Dienstleistungen ihrer Behörde wesentlich positiver bewerten und gleichzeitig weniger Nutzungshemmnisse sehen als Nichtnutzer. Aus diesem Grund sind Möglichkeiten und Anreize zur Sammlung von E-Government-Nutzungserfahrungen zu intensivieren bzw. zu unterstützen (o. V. 2011b, 8ff).

Kritische Erfolgsfaktoren zur Akzeptanzförderung von eID-Projekten

Aus einer umfassenden Literaturrecherche lassen sich insbesondere die folgenden kritischen Erfolgsfaktoren ableiten:

Innovationsbezogene Faktoren:

(1) Keine zentrale Datenbank: Dieses Thema wurde in letzter Zeit in den Medien sehr oft diskutiert, und die Kommentare der Bürger bezüglich dieser Berichte machen deutlich, dass sie digitale Ausweise, die biometrische Daten beinhalten, als eine Gefahr der zentralen Speicherung von persönlichen Daten wahrnehmen.

(2) Infrastruktur mit optimaler Sicherheit: Die Sicherheit der Authentifizierung ist eine der entscheidendsten Fragen. Wie oben diskutiert wurde, gibt es verschiedene Risiken, die mit falscher Identifikation von Nutzern in Verbindung stehen. Eine Methode zur Verbesserung ist die Gewährung von Garantien durch vertrauenswürdige Dritte.

(3) Biometrie: Für die Endnutzer ist der Aspekt der Biometrie eines der wichtigsten Bedenken bei solchen Projekten. Um die Akzeptanz des Projekts zu verbessern und Vertrauen zu schaffen, sollte Biometrie nur von der Regierung und nur bei vorher definierten Fällen, die höchste Sicherheit erfordern (wie z. B. Grenzkontrollen), verwendet werden.

Nutzerbezogene Faktoren:

(4) **Gezielte Kommunikation:** Es wird oft dazu geraten, Kommunikation zur Schaffung von Akzeptanz und Vertrauen bei der Einführung einer neuen Technologie zu verwenden (Zerfaß 2009, 23ff). Für den Erfolg eines landesweiten Projekts, wie dem nPA-Projekt, ist die Rolle der Medien entscheidend. Die Regierung sollte ihre Kommunikation insbesondere auf Themen ausrichten, auf die Bürger empfindlich reagieren. Ausgehend von unserer empirischen Recherche, sind die Privatsphäre der Menschen, die Angst nummeriert und kategorisiert zu werden und die Bedenken bezüglich der Übertragungssicherheit hier Hauptaspekte. Nachdem diese analysiert wurden, schlagen wir vor, dass die Regierung ihre Kommunikation anhand von diesen Aspekten ausrichtet.

(5) **Vorstellung von Vorteilen bei der Nutzung von digitalen Ausweisen:** Die Kosten-Nutzen-Analyse ist eine Methode zur Bewertung der Wirtschaftlichkeit von verschiedenen Alternativen, um zu sehen, ob die erwarteten Vorteile die Kosten überwiegen. In gleicher Weise gibt es zahlreiche Methoden zur Analyse von Vorteilen und Risiken, die mit einer Entscheidung verbunden sind.

(6) **Entscheidung, Daten zu übermitteln:** Da alle Daten in digitalen Ausweisen persönliche Daten sind, sollten die Ausweisbesitzer immer die Kontrolle darüber haben, welche Daten übertragen werden sollen und wer Zugriff darauf hat. Nicht autorisierter Zugang zu Daten auf digitalen Ausweisen sollte unter keinen Umständen erlaubt werden.

Der Übergang von Verwaltungsorganisation und Dienstleistungsangebot von klassischen zu neuen Formen birgt technische und soziale Risiken. An erster Stelle ist beim nPA zu beachten, dass die zentrale Speicherung von biometrischen Daten als Gefahr gesehen wird. In anderen Ländern wird deshalb darauf verzichtet. Es ist von kritischer Bedeutung, dass diese zentrale Datenbank sehr sicher und zuverlässig ist. Die Zuverlässigkeit ist auch bei dem Prozess des elektronischen Identitätsnachweises ein wichtiger Erfolgsfaktor. Die gegenseitige Authentifizierung von Dienstleistungsanbieter und -nachfrager muss bestmögliche Sicherheit gewährleisten, was durch Partnerschaften mit Dritten garantiert werden kann. Wissenschaftliche Studien und das technische Know-how von Unternehmen tragen dazu bei, diesen Prozess zuverlässiger zu gestalten. Wichtig ist jedoch, dass die Anwendungen von Bürgern auch subjektiv als sicher empfunden werden. Dazu zählen vorher definierte Berechtigungen zur Nutzung von elektronischen und biometrischen Daten des nPA, die Kontrolle über den Zugriff auf diese Daten seitens der Inhaber und außerdem die Dokumentation der ergriffenen Maßnahmen. Vertrauen ist ein zentraler Erfolgsfaktor. Die Rolle der Medien und die Aussagen der Regierung über den nPA sind ausschlaggebend für die kommunikative Erzeugung von Vertrauen.

3. eID-Projekte in Europa

Deutschland ist nicht das erste Land, das einen digitalen Ausweis einführt. Zehn europäische Länder haben bereits nationale elektronische Ausweiseprojekte eingeführt und dreizehn weitere haben dies beschlossen und planen zurzeit die Einführungen (siehe Anhang B). Dies bietet Deutschland die Möglichkeit, die Herausforderungen, die diese Länder hatten, zu analysieren sowie von ihren Erfahrungen, besonders in Bezug auf die technischen Möglichkeiten, zu lernen.

Bis 2009 sollten alle EU-Mitgliedsstaaten ihre elektronischen Reisedokumente mit einem digitalen Passfoto und zwei Fingerabdrücken erweitern. Mit dem „European Citizen Card" (ECC)-Projekt gibt es erste Schritte zur Einführung einer einzigen Karte für alle Transaktionen der Bürger. Die ECC enthält einen Chip, der persönliche Daten, ein digitales Foto und zwei Fingerabdrücke speichert. Digitale Signaturen sind bei der „European Citizen Card" optional. Eine große Herausforderung ist die notwendige Systeminteroperabilität. Ausweisdokumente aus allen Ländern sollen in allen EU-Staaten lesbar sein. Obwohl die meisten EU-Länder schon Ausweisprogramme gestartet haben, benutzen die meisten die ECC-Spezifikationen noch nicht.

In Europa gibt es nicht viele Studien, die sich mit den sozialen Aspekten bei nationalen Ausweisen beschäftigen. Allerdings hängen soziale Aspekte zum Teil von kulturellen Normen ab, die sich von Land zu Land unterscheiden. Deshalb sollten Studien, die sich auf soziale Aspekte konzentrieren, für jede Kultur einzeln und gezielt durchgeführt werden.

Auffällig ist: Unsere umfangreiche Literaturanalyse und internetbasierte Recherche zeigt, dass der Vertrauensaspekt im Zusammenhang mit digitalen Ausweis-Projekten nicht herausgehoben diskutiert wurde. Obwohl viele Länder die Bedeutung der Sicherheit der Infrastruktur betonen, fanden wir keine Informationen über die wahrgenommene Rolle des Vertrauens bzw. über ergriffene Maßnahmen zudessen Steigerung.

3.1. Internationaler Vergleich von eID-Infrastrukturen

In allen europäischen Ländern wird auf eine Verwaltungsmodernisierung hingewirkt (Assar 2011, 85). Dies wird in Abbildung 10 konkreter erläutert.

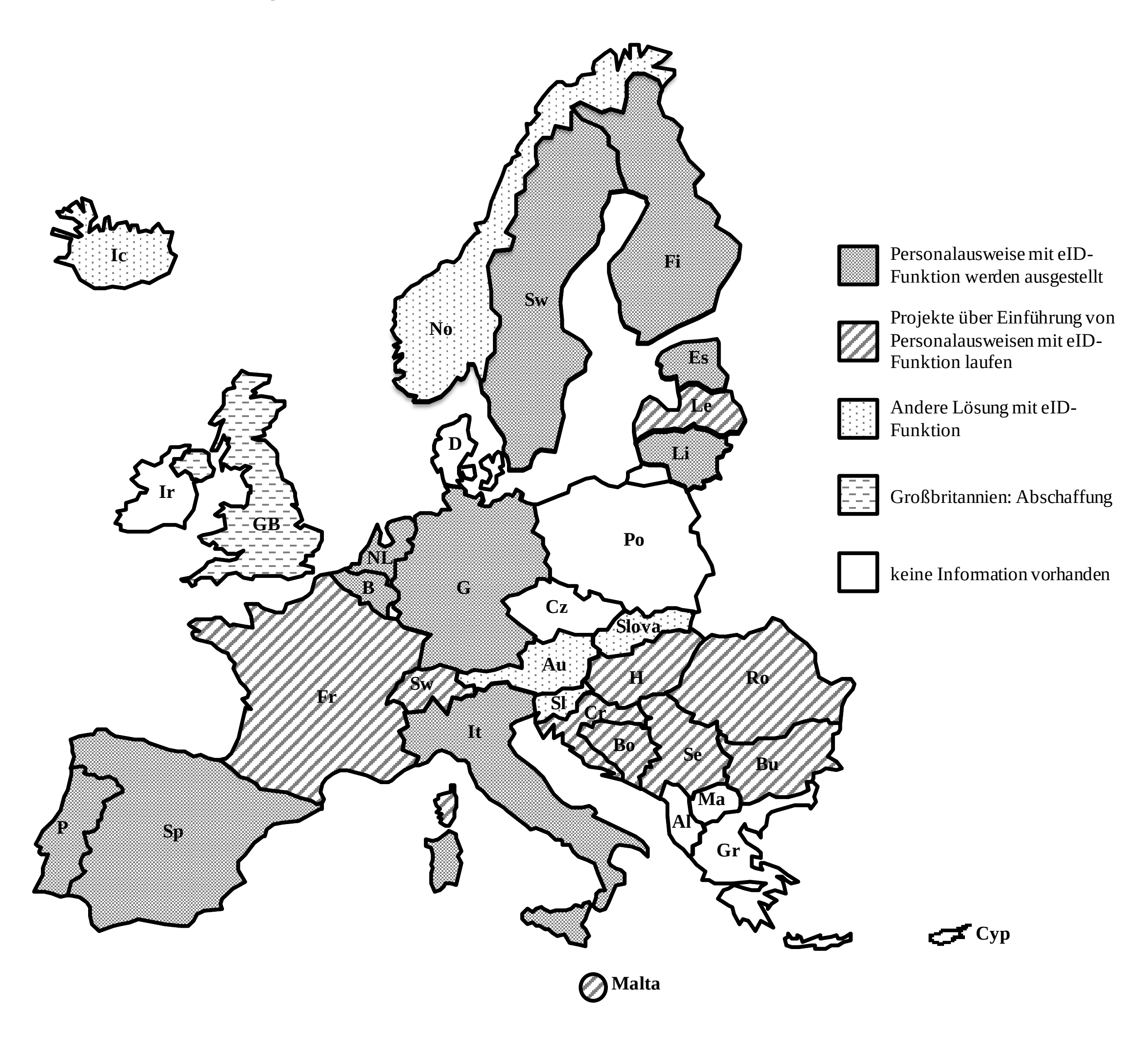


Abbildung 10: EU-weiter Status der Einführung von Personalausweisen mit eID-Funktion (Quelle: Eigene Darstellung in Anlehnung an (Assar 2011, 85)

Der technologische Fortschritt, die Globalisierung und die Entwicklung der Gesellschaft treiben diese Modernisierung voran. Obwohl jedes Land den Einführungsprozess von E-Government-Projekten unterschiedlich abwickelt, stellen europäische Harmonisierungsbestrebungen sicher, dass an alle Länder gleiche Anforderungen gestellt werden. So sind die einzelnen Staaten vergleichbar und unterscheiden sich grundsätzlich nur im Zeitrahmen und dem operativen Vorgehen (Assar 2011, 85). Dies macht einen Ländervergleich beim Thema nPA sinnvoll.

Um die Entwicklung des Marktes für neue Personalausweise im europäischen Raum verstehen zu können, wird zunächst die allgemeine Ausweispflicht untersucht. Nach diesem Kriterium gliedern sich die europäischen Länder in drei Gruppen mit folgenden Besonderheiten: keine Ausweispflicht der

Bürger und kein Personalausweis erhältlich, keine Ausweispflicht trotz eingeführter Identitätskarte und Ausweispflicht und zur Verfügung stehende Identitätskarten.

Keine Identitätskarte:

In manchen europäischen Ländern gab es vor der Einführung der neuen Personalausweise weder Identitätskarten noch die gesetzliche Grundlage dafür. Als Identitätsnachweis wurde dagegen der Führerschein und als Reisedokument der Reisepass genutzt. In einigen Ländern wurde dennoch an der Einführung eines neuen Personalausweises gearbeitet, wie zum Beispiel in Großbritannien (Fawer 2009, 18).

Identitätskarte vorhanden, keine Ausweispflicht:

In anderen Ländern hingegen stand bereits vor der Einführung der elektronischen Identitätsnachweise ein Personalausweis zur Verfügung, eine Ausweispflicht ist allerdings nicht gesetzlich verankert. Beispiele dafür sind Finnland und Österreich (Stevens et al. 2010, 29; Fawer 2009, 18).

Identitätskarte für alle Bürger, Ausweispflicht:

In anderen Ländern haben Bürger eine gesetzlich geregelte Ausweispflicht und dementsprechend stehen ihnen auch Personalausweise zur Verfügung. Vertreter dieser Gruppe sind bspw. Deutschland, Spanien und Belgien (Stevens et al. 2010, 29; Fawer 2009, 18).

Im Folgenden wird exemplarisch auf Ausweis-Projekte aus Belgien, Großbritannien, Finnland, Österreich und Spanien eingegangen. Österreich hat bereits eine virtuelle Bürgerkarte eingeführt (Bundeskanzleramt Österreich 2005), Finnland ist eines der ersten Länder weltweit, die elektronische Ausweise haben und hat deshalb viel Erfahrung auf diesem Gebiet (Schmeh 2009, 185). In Belgien ist die Belgien Personal Identity Card bereits sehr weit verbreitet (Assar 2011, 74; Schmeh 2009, 180), Spanien ist das beste Beispiel in Bezug auf Datensicherheit und -transfers (Assar 2011, 82). Großbritannien hingegen dient als Beispiel dafür, dass die Zukunft einer eID-Karte auch von der jeweiligen Regierung abhängen kann. Aufgrund der genannten Merkmale kann man aus der Betrachtung der ausgewählten Länder Konsequenzen für Deutschland herleiten. Untersucht werden Rahmenbindungen, rechtliche Vorschriften, auf dem Ausweis gespeicherte Daten und die Verwendung des Ausweises im jeweiligen Land. Anschließend werden die wichtigsten Fakten der genannten Projekte nochmals tabellarisch zusammengefasst.

3.1.1.Belgien

Rahmenbedingungen

„Belgien zählt zu den weltweiten Vorreitern im Bereich der elektronischen Identitätskarten“ (Schmeh 2009, 180). Nach Finnland und Estland ist Belgien chronologisch der dritte europäische Staat, der seinen Bürgern elektronische Identitätskarten zur Verfügung stellt (Schmeh 2009, 181). Des Weiteren wird mit der Belgien Personal Identity Card (BELPIC) auch die Verwendung einer elektronischen Signatur angeboten, die in manchen E-Government-Anwendungen nötig ist, aber auch als Zugangsvoraussetzung für Chatforen genutzt wird. Somit sorgt die Verwaltung für verbesserten Jugendschutz im Internet (z. B. bei Safer Chat). Belgien ist einer der E-Ausweis-Pioniere und BELPIC wurde dementsprechend vor der Festlegung des MRTD (Machine Readable Travel Dokument) Standards entwickelt. Der Standard sorgt dafür, dass die Personalausweise eine aufgeprägte maschinenlesbare Zone sowie einige Besonderheiten am Chip aufweisen. Da BELPIC vor Festlegung des Standards entworfen wurde, wurde nachträglich nur der Aufdruck hinzugefügt, der Chip jedoch nicht geändert (Schmeh 2009, 181f). Dies bedeutet, dass BELPIC nicht MRTD-konform ist, also nicht die standardisierte Gestaltung der E-Ausweise EU-weit hat, was den EU-Harmonisierungsbestrebungen in diesem Bereich entgegenwirkt (Schmeh 2009, 181f).

Rechtliche Vorschriften

In Belgien sind alle Bürger, die das zwölfte Lebensjahr vollendet haben, verpflichtet, den neuen Personalausweis zu besitzen. Weiter gibt es für Kinder, die jünger als zwölf Jahre sind, ein freiwilliges Äquivalent namens Kids-ID. Ab dem fünfzehnten Lebensjahr gibt es auch strenge Mitführpflicht, es sei denn, der Bürger befindet sich innerhalb einer Entfernung von nicht mehr als 200 Meter zu dessen Wohnsitz (Stevens et al. 2010, 21; Schmeh 2009, 180f). Im Ausland wohnende Bürger haben ebenso einen Anspruch auf BELPIC. Seit 2004 ist die Karte in Belgien erhältlich (Assar 2011, 72) und seit 2009 auch in den belgischen Konsulaten im Ausland (Stevens et al. 2010, 21). Dadurch wird erleichtertes Reisen in- und außerhalb Belgiens erzielt, sowie die Vereinfachung der administrativen Prozesse, wenn Bürger temporär oder permanent nach Belgien ziehen.

Auf dem Ausweis gespeicherte Daten

Auf der kontaktbehafteten Identitätsnachweiskarte werden die Daten des Inhabers teilweise in aufgedruckter Form und vollständig in elektronischer Form gespeichert. Name, Nationalität, Geburtsdatum und -ort, Kartennummer, Passfoto, Unterschrift und Identifikationsnummer des Inhabers sind sowohl aufgedruckt als auch auf dem Chip gespeichert. Zu den elektronischen Daten zählen auch noch die Adresse des Bürgers und seine elektronische Signatur. Biometrische Daten werden hingegen nicht auf dem BELPIC gespeichert (Schmeh 2009, 182).

Verwendung

In Belgien wird eine breite Palette von Dienstleistungen angeboten, die den Identitätsnachweis durch BELPIC verlangen. Beispiele dafür sind Bildung, Gesundheitsdienstleistungen, Personenverkehr und Immobiliengeschäfte (Stevens et al. 2010, 21). 8.3 Mio. von insgesamt 10.4 Mio. Bürger verfügen über BELPIC. Aufgrund der breiten Nutzung ermutigt die Verwaltung die Verkäufer, das Kartenlesegerät in alle neuen Heimcomputer einzubauen (Stevens et al. 2010, 22).

3.1.2.Großbritannien

Rahmenbedingungen

Im Jahr 2006 beschloss die Regierung von Großbritannien ein Gesetz einzuführen (Identity Cards Act/Bill), das die Einführung des neuen Personalausweises (Identity Card) regelt. Dieses war von Beginn an sehr umstritten und erst zwei Jahre nach der Erstfassung wurde eine Kompromisslösung gefunden (Sullivan 2010, 1). Einige Zeit arbeitete die Labour-Regierung an der raschen Einführung der Identity Card (Schmeh 2009, 191). Im Mai 2010 jedoch beschloss die beim Regierungswechsel gewählte konservativ-liberaldemokratische Koalition die Abschaffung der ID Card, des National Identity Register (NIR) und der ID Card von Bürgern des Europäischen Wirtschaftsraums. Die Identity Card ist seit Januar 2011 kein rechtsgültiges Dokument mehr und das NIR wird im Februar 2011 abgeschaltet (Home Office 2011).

Im Folgenden werden die ursprünglichen Ziele der Labour-Regierung, die durch die Einführung der Identity Card erreicht werden sollten, erläutert. Durch die Einführung der Identity Card sollte vor allem das Bedürfnis nach Sicherheit gestillt werden. Mit der Speicherung der biometrischen Daten auf dem Chip sollte erzielt werden, dass Identitätsdiebstahl durch ähnlich aussehende Personen beseitigt wird. Weiter sollten die elektronischen Identitätskarten und das NIR sicherstellen, dass niemand (insbesondere auch Kriminelle und Terroristen) multiple Identitäten besitzt. Als Nächstes wurde geplant, die Identity Card auch für öffentlichen Dienstleistungen einzusetzen, um alle damit verbundenen Vorteile nutzen zu können (Home Office 2010c).

Rechtliche Vorschriften

Identity Cards für englische Bürger wurden 2009 den Bewohnern von Greater Manchester zur freiwilligen Nutzung zur Verfügung gestellt. Es wurde geplant, diese bis 2012 allen Bürgern anbieten zu können (Home Office 2010a). Im Jahr 2012 sollte die Aufnahme von Daten und die Erstellung eines Eintrags ins NIR für jeden Bürger, der sein sechzehntes Lebensjahr vollendet hat, bei Beantragung eines Reisepasses und ab 2017 für alle Bürger verpflichtend sein (Sullivan 2010, 2). Diese Vorschrift wurde mit der Abschaffung der Infrastruktur ebenfalls widerrufen (Home Office 2011).

Auf dem Ausweis gespeicherte Daten

Die Nutzung der britischen Identity Card für E-Government-Dienstleistungen war nicht vorgesehen. Deswegen sollte der Identitätsnachweis über keine elektronische Signatur verfügen (Schmeh 2009, 192). Lange vor Entwicklung des neuen Personalausweises, waren E-Government-Dienstleistungen im Internet für Bürger und Wirtschaftsakteure über das Portal http://www.gateway.gov.uk/ zugänglich.

Ziel der Einführung war, eine sichere und zuverlässige Identifizierung des Ausweisinhabers zu entwickeln und auf diese Weise die nationale Sicherheit zu verbessern. Die Daten der Bürger wurden zum Teil auf der Identity Card und vollständig in der Online-Datenbank NIR gespeichert. Über jeden Bürger wurde im NIR ein Eintrag mit folgenden Daten eingerichtet: persönliche Informationen, Identifizierungsinformationen, Aufenthaltsstatus, Kennnummern, Eintragshistorie, Karten- und Registrierungshistorie, biometrische Daten, Überprüfungsinformationen über die Echtheit des Eintrags, Sicherheitsinformationen zum Zugriff auf die Daten und Logdaten über Chronologie der Datenzugriffe. Ein Teil dieser Informationen sowie die biometrischen Daten sollten auf dem Chip der Identity Card gespeichert werden (Home Office 2010c; Schmeh 2009, 192).

Verwendung

Für den Zugriff auf die Daten eines Bürgers muss man zunächst eine Berechtigung haben. Die Informationen sollten mittels einer Online-Verbindung zwischen der Identity Card und dem NIR aufgerufen werden. Dazu benötigte man allerdings das Einverständnis des Bürgers, da dieser seine PIN eingeben sollte, um den Vorgang zu ermöglichen. Es war vorgesehen, dass eine Änderung der Daten nur bei den zuständigen Behörden möglich wäre. Die Identity Card sollte als Identitätsnachweis bei Polizei, Behörden und im privatwirtschaftlichen Bereich dienen. Beispiele sind die Kontoeröffnung bei einer Bank, Mietverträge und Vereinbarungen einer Ratenzahlung. (Schmeh 2009, 192). Weiter gab es vor Januar 2010 die Möglichkeit die Identity Cards als Reisedokument zu verwenden (Home Office 2010b, 2011).

Im Mai 2010 wurde verkündigt, dass die Identity Card und das NIR abgeschafft sowie alle bisher im NIR vorhandenen Daten gelöscht werden. Als Grund dafür wurde die Bedeutung des Gleichgewichts zwischen der nationalen Sicherheit und Bürgerrechten angegeben (Home Office 2010b).

3.1.3.Finnland

Rahmenbedingungen

Finnland ist (nach Brunei) der zweite Staat der Welt, der einen elektronischen Identitätsnachweis einführte. Dieser heißt FINEID (sprich „fin-i-ai-di“) und wird seit 1999, zusätzlich zum Personalausweis ohne Chip, an die Bürger ausgegeben (Schmeh 2009, 185).

Rechtliche Vorschriften

Finnische Bürger sind nicht verpflichtet die FINEID zu besitzen, da in Finnland keine Ausweispflicht besteht. Viele Bürger nutzen neben ihrem Reisepass oder Führerschein, auch den Personalausweis ohne Chip um sich auszuweisen. FINEID ist ebenfalls für Firmen ausstellbar. Im Jahr 2003 verfügten 16.000 der insgesamt 5 Mio. Firmen über einen elektronischen Identitätsnachweis in Form des FINEID, bis 2005 waren es 53.000 (Schmeh 2009, 185).

Auf dem Ausweis gespeicherte Daten

Auf der kontaktbehafteten Chipkarte werden neben Name und Geschlecht, die Ausweisnummer, die Nationalität, das Geburtstagsdatum, die Sozialversicherungsnummer, Angaben über die Gültigkeitsdauer des Ausweises und eine eigenhändige Unterschrift des Inhabers aufgedruckt (Schmeh 2009, 186ff). FINEID beinhaltet als elektronische Daten nur die Vor- und Nachnamen des Inhabers (Schmeh 2009, 186ff), Signaturzertifikate und kryptografische Daten (Assar 2011, 80). Diese kryptografischen Daten sind zwei private Schlüssel und das zugehörige Zertifikat. Jeder dieser Schlüssel ist 1.024 Bit lang und kann nur mit einer PIN genutzt werden. Der eine Schlüssel dient der Authentifizierung und Verschlüsselung, während der andere für die elektronische Signatur verwendet wird (Schmeh 2009, 187).

Verwendung

Als die Anzahl der FINEID Besitzer nicht hoch war, gab es nicht viele Anwendungen und dementsprechend kein großes Interesse seitens der Bürger. Inzwischen ist die Anzahl der ausgestellten Ausweise deutlich angestiegen und folglich gibt es ein breiteres Angebot an Anwendungsmöglichkeiten (Schmeh 2009, 185). Weiterhin ist die Nutzung von Dienstleistungen mittels FINEID nicht nur vom heimischen PC mit Kartenlesegerät und Internetzugang möglich, sondern auch an Kartenautomaten, die durchgehend betriebsbereit und zugänglich sind. Bürger können bei der Polizei die Speicherung dieser Zertifikate auf ihren Bankkarten, SIM-Karten, im beruflichen Leben verwendeten Karten usw. beantragen (Assar 2011, 80). Somit kann zum Beispiel ein Bankkonto im Internet verwaltet werden, ohne dass TAN-Serien mitgeführt werden müssen. Wenn der Nutzer die Zertifikate nutzt, kann er Transaktionen verwalten und mit der elektronischen Signatur können Verträge online unterzeichnet

werden, wie bspw. ein Darlehnsvertrag. Des Weiteren ist auch die Verwendung für E-Government-Dienstleistungen möglich (Assar 2011, 81).

3.1.4.Österreich

Rahmenbedingungen

Mit der Bürgerkarte wird in Österreich daran gearbeitet, dass alle Behördengänge online erledigt werden können, was durch Orts- und Öffnungszeitunabhängigkeit und Zeitersparnis zur Verwaltungsmodernisierung führt (Roßnagel/Yildirim 2002, 161).

Das Konzept des elektronischen Identitätsnachweises in Österreich unterscheidet sich von anderen Projekten, die in diesem Abschnitt betrachtet werden. Die sogenannte Bürgerkarte ist keine physische Karte, sondern deren virtuelle Repräsentation. Sie kann auf verschiedene Trägermedien geladen werden, solange diese chipbasiert sind bspw. auch auf SIM-Karten und Bankkarten (Bundeskanzleramt Österreich 2005). Die Bürgerkarte wird bei der Ausstellung der e-card, die eine Gesundheitskarte ist, kostenfrei geladen. Die Aktivierung der Bürgerkarte bleibt jedoch dem Bürger überlassen (Bundeskanzleramt Österreich 2010). Dadurch wird sichergestellt, dass jeder Bürger über eine signaturfähige Karte verfügt. Das führt dazu, dass alle (8 Mio.) österreichischen Bürger über einen elektronischen Identitätsnachweis verfügen (Roßnagel/Yildirim 2002, 161). Die Aktivierung und Nutzung der Bürgerkarte auf der SIM-Karte des Mobiltelefons ist kostenfrei, mit Ausnahme der Roaminggebühren, falls sich der Bürger im Ausland befindet (Bundeskanzleramt Österreich 2010).

Das Konzept der Bürgerkarte wurde im Dezember 2005 im Bereich ‚Best Practices‘ für Datenschutz in der europäischen öffentlichen Verwaltung ausgezeichnet. Grund dafür ist die Umsetzung der Grundrechte der Bürger und Datenschutz „in hervorragender Weise“ (Bundeskanzleramt Österreich 2005).

Rechtliche Vorschriften

Die Bürgerkarte wird seit 2002 (Gerstbach 2004, 8) mit Vollendung des vierzehnten Lebensjahres auf freiwilliger Basis ausgestellt. Auch Ausländer, die in Österreich gemeldet sind oder Österreicher, die nicht länger als zehn Jahre im Ausland wohnen, bekommen Einträge im Zentralen Melderegister (ZMR). Zusätzlich gibt es ein ‚Ergänzungsregister für natürliche Personen‘. Dadurch können all diejenigen österreichischen Staatsbürger, die nicht im ZMR gemeldet sind, eine Bürgerkarte beantragen (Bundeskanzleramt Österreich 2010).

Die Bürgerkarte ermöglicht eine elektronische Vollmacht. Jeder Bürger kann anderen Personen Vollmacht bei der Stammzahlenregisterbehörde erteilen. Dieses Vollmacht wird auf die Infobox, einem Speicherbereich der Bürgerkarte, des Bevollmächtigten übertragen. Eine Vertretungsvollmacht für ein

Unternehmen ermöglicht, dass natürliche Personen im Namen eines Unternehmens handeln können. Aufgrund der gesetzlichen Vollmachtregelung können Eltern mit ihrer eigenen Bürgerkarte im Namen ihrer minderjährigen Kinder unterschreiben (Bundeskanzleramt Österreich 2010).

Auf dem Ausweis gespeicherte Daten

Für die Bürgerkarte werden keine biometrischen Daten erfasst. Diese werden lediglich auf dem elektronischen Reisepass gesichert und sind für Reisen, vor allem in die USA, vonnöten (Schmeh 2009, 163).

Die Bürgerkarte bietet eine sichere elektronische Signatur an, die durch kryptografische Verfahren ermöglicht wird. Die dafür notwendigen Schlüssel und Zertifikate werden auf der Bürgerkarte gespeichert und somit auf alle Datenträger, auf denen sie aktiviert ist, übertragen. Jedoch genügen diese Daten nicht, um eindeutig und verbindlich eine Person elektronisch zu identifizieren. Deswegen sorgt ein Bereich der Bürgerkarte explizit für diese Personenbindung. Dies wird durch die Speicherung der Stammzahl erreicht. Die Stammzahl ist der eindeutige geheime Schlüssel, der von der Stammzahlenregisterbehörde aus der Melderegisterzahl abgeleitet wird. Die Melderegisterzahl ist die Nummer des Eintrags in der ZMR. Somit wird die Bürgerkarte mit den Daten im ZMR verbunden, ohne dass die Daten des Bürgers direkt auf den Chip gespeichert werden. Da der Aufruf dieser Informationen über die Stammzahlenregisterbehörde erfolgt, ist der Eintrag im ZMR nicht von Außen angreifbar. Des Weiteren erfolgt bei elektronischen Verfahren im Bereich E-Commerce und E-Government die Identifikation nicht durch die Stammzahl, sondern durch das bereichsspezifische Personenkennzeichen (bPK). Das ist eine von der Stammzahl abgeleitete Zahl, die nur den Zugang zu den notwendigen Daten erlaubt. So ist bspw. das bPK im Bereich Steuern und das bPK im Bereich Bauen nicht nur verschieden, sondern auch nicht voneinander ableitbar. Ebenfalls ist es unmöglich, aus einem oder mehreren bPK die Stammzahl abzuleiten (Gerstbach 2004, 2ff).

Die Bürgerkarte hat weitere Speicherbereiche, Infoboxen genannt, auf denen die Vollmachtsdaten oder auch andere für Verwaltungsvorgänge nötige Daten gespeichert und aktualisiert werden. Bei Nutzung verbinden sich die Infoboxen mit einer externen Datenbank und bieten somit den Vorteil, dass unabhängig von Verwendungsort und Datenträger die Daten immer vollständig und aktuell sind. Außerdem ist so die Datenmenge unabhängig von der Speicherkapazität des Chips. Hierbei sorgen wiederum sämtliche Verschlüsselungsverfahren für die Vertraulichkeit der Daten (Bundeskanzleramt Österreich 2010; Gerstbach 2004, ff).

Verwendung

Den Bürgern werden kostenpflichtige Kartenlesegeräte angeboten, um die Nutzung der Bürgerkarte zu fördern. Durch die Nutzung der e-card und eines Kartenlesegeräts können E-Mails elektronisch signiert werden. Zudem ermöglicht die Bürgerkarte den Identifikationsnachweis sowohl bei E-

Government-Dienstleistungen als auch gegenüber der Wirtschaft wie zum Beispiel beim Online-Banking statt PIN- und TAN-Nummern. Weiter können österreichische Bürger mehrere Karten als Bürgerkarten aktivieren und diese parallel nutzen. Bei einem Verlust oder Diebstahl einer dieser Datenträger bleibt die Bürgerkarte geschützt, da sie einerseits nur bei Eingabe einer PIN-Nummer aufrufbar ist, andererseits man dies gleich melden kann, was zu einem unumkehrbaren Widerruf der Zertifikate führt. Dann muss der Bürger neue Zertifikate auf seine Karten laden und aktivieren lassen und die verlorene Karte bleibt unbrauchbar (Bundeskanzleramt Österreich 2010).

3.1.5.Spanien

Rahmenbedingungen

In Spanien wurde der elektronische Identitätsnachweis (Documento Nacional de Identidad – DNI bzw. DNIe) im Jahr 2006 eingeführt. Bis März 2007 wurden etwa 420.000 dieser Karten ausgestellt (Stevens et al. 2010, 25f) und bis Ende 2009 etwa 13 Mio. (Assar 2011, 82).

Rechtliche Vorschriften

In Spanien besteht zwar eine Ausweispflicht, jedoch keine Mitführpflicht. Bei Aufforderung durch die Polizei muss der Bürger seinen Ausweis vorzeigen, kann jedoch den Polizisten zum Aufbewahrungsort des Ausweises bitten. Die Beantragung eines DNIe ist seit seiner Einführung verpflichtend für alle Bürger, die das vierzehnte Lebensjahr vollendet haben (Stevens et al. 2010, 25).

Auf dem Ausweis gespeicherte Daten

Auf dem DNIe werden die für einen Lichtbildausweis typischen Daten aufgedruckt. Hierzu gehören Name, Geburtsdatum, Geschlecht, Nationalität, Ausweisnummer (diese behält der Bürger lebenslang), Seriennummer (die sich bei Erneuerung des Ausweises ändert), Geburtsdatum und -ort, Wohnort und Name der Eltern. Weiter enthält der Ausweis eine MRTD-standardisierte maschinenlesbare Zone die eine Nutzung des Ausweises als Reisedokument erlaubt (Schmeh 2009, 208f).

Neben den gedruckten Daten wird auf dem DNIe eine elektronische Signatur gespeichert (Stevens et al. 2010, 26). Der Chip beinhaltet zwei elektronische Zertifikate (einen für den Identitätsnachweis und einen für die elektronische Signatur) sowie zwei private und einen öffentlichen Schlüssel (Schmeh 2009, 209f). Die Zertifikate sind nach europäischen Standards entworfen, sodass der DNIe EU-weit verwendet werden kann. Weiter werden von den Bürgern bei der Ausstellung dieser Karte Fingerabdrucke erfasst. Die Daten werden auf dem Chip des Ausweises und in einer zentralen Datenbank gespeichert (Schmeh 2009, 209).

Die Authentifizierung der Bürger erfolgt mithilfe einer zentralen Datenbank, in der persönliche Daten, Lichtbild und ein Fingerabdruck gespeichert sind. Alle Datentransfers und Zugriffe auf diese Datenbank werden verfolgt, um die Datenbank und die Daten zu schützen. Dies wird strikt durch die nationale Datenschutzbehörde Spaniens, die AEPD (Agencia Española de Protección de Datos) kontrolliert) überwacht. In Spanien wird hoher Wert auf das Management persönlicher Daten gelegt. Zum Beispiel sind die genauen Sicherheitsvorkehrungen zum Schutz personenbezogener Daten gesetzlich bestimmt (Stevens et al. 2010, 26).

Verwendung

Der DNIe wird für eine breite Palette an Anwendungen genutzt. Beispiele für privatwirtschaftliche Dienstleistungen sind Antragstellung für ein Darlehen oder eine Bankkontoeröffnung (Stevens et al. 2010, 25). E-Government-Dienstleistungen werden ebenfalls angeboten (Schmeh 2009, 210). Für den Identitätsnachweis wird die Karte von einem Kartenlesegerät ausgelesen. Erst wenn eine elektronische Signatur erstellt werden soll, muss der Bürger seine PIN-Nummer eingeben (Assar 2011, 82). Spanische Bürger können durchgehend an Terminals in Polizeidienststellen die elektronisch gespeicherten Daten überprüfen, die PIN ändern und die Gültigkeit der Zertifikate überprüfen bzw. verlängern (Assar 2011, 82).

3.1.6.Zusammenfassung

Die Verwaltungen in den EU-Staaten entscheiden sich für verschiedene Konzepte bei der Einführung von neuen Personalausweisen. Eine Zusammenfassung der eben erläuterten Konzepte in den fünf repräsentativen Ländern und in Deutschland erfolgt in Tabelle 6. Im folgenden Kapitel werden diese Unterschiede und Gesetzmäßigkeiten analysiert, um daraus Erkenntnisse über den nPA in Deutschland zu gewinnen.

Staat	Kennzahlen	Rechtliche Vorschriften	Infrastruktur und Biometrie	Verwendung
Großbritannien	61 Mio. Bürger; Keine Angaben über Anzahl ausgestellter Identity Cards seit der Einführung im Jahr 2009 (Stand: 2010).	Keine Ausweispflicht Keine Mitführpflicht Verwendung als Reisedokument möglich	Keine Kartenlesegeräte Keine elektronische Signatur Biometrischen Daten Zentrale Datenbank (NIS)	E-Government – nein Privatwirtschaftlich – ja E-Banking – keine Angaben

Staat	Kennzahlen	Rechtliche Vorschriften	Infrastruktur und Biometrie	Verwendung
Österreich	8.1 Mio. Bürger; Etwa 8 Mio. ausgestellte Bürgerkarten seit der Einführung im Jahr 2002 (Stand: 2008).	Keine Ausweispflicht Keine Mitführpflicht Verwendung als Reisedokument nicht möglich, da virtuelle Karte	Kartenlesegeräte Elektronische Signatur Keine biometrischen Daten Zentrale Datenbank (ZMR)	E-Government – ja Privatwirtschaftlich – ja E-Banking – ja
Finnland	5.2 Mio. Bürger; 0.275 Mio. ausgestellte FINEID seit der Einführung im Jahr 1999 (Stand: 2009).	Ausweispflicht Mitführpflicht Verwendung als Reisedokument möglich	Kartenlesegeräte Elektronische Signatur Biometrische Daten – keine Angaben Zentrale Datenbank – keine Angaben	E-Government – ja Privatwirtschaftlich – ja E-Banking – ja
Belgien	10.4 Mio. Bürger; 8.3 ausgestellte BELPIC seit der Einführung im Jahr 2004 (Stand: 2009).	Ausweispflicht Mitführpflicht Verwendung als Reisedokument möglich	Kartenlesegeräte Elektronische Signatur Keine biometrische Daten Zentrale Datenbank – keine Angaben	E-Government – ja Privatwirtschaftlich – ja E-Banking – ja
Spanien	42.5 Mio. Bürger; 13 Mio. ausgestellte DNIe seit der Einführung im Jahr 2006 (Stand: 2009).	Ausweispflicht Mitführpflicht Verwendung als Reisedokument möglich	Kartenlesegeräte Elektronische Signatur Biometrische Daten - Fingerandrücke Zentrale Datenbank	E-Government – ja Privatwirtschaftlich – ja E-Banking – ja

Staat	Kennzahlen	Rechtliche Vorschriften	Infrastruktur und Biometrie	Verwendung
Deutschland	82.6 Mio. Bürger; Keine Angaben über Anzahl ausgestellte nPA seit der Einführung im Jahr 2010 (Stand: 2010).	Ausweispflicht Keine Mitführpflicht Verwendung als Reisedokument möglich	Kartenlesegeräte Elektronische Signatur Biometrische Daten Zentrale Datenbank	E-Government – ja Privatwirtschaftlich – ja/geplant E-Banking – evtl. in der Zukunft

Tabelle 6: Zusammenfassung des Ländervergleichs (Quelle: Eigene Darstellung)

3.1.7.Folgerungen hinsichtlich des Marktpotenzials

Aus dem Ländervergleich gewinnt man zahlreiche Informationen über mögliche Sicherheitsbedenken bei der europaweiten Verwendung des neuen Personalausweises. Daraus können Schlussfolgerungen über potenzielle zukünftige Sicherheitsprobleme bei der Verwendung neuer Personalausweise in Deutschland gezogen werden. Aus der Betrachtung des Umgangs anderer Länder mit der Datensicherheit werden Anforderungen an den nPA/die AusweisApp abgeleitet.

In Europa werden sowohl kontaktlose (z. B. in Deutschland und in der Schweiz) als auch kontaktbehaftete (z. B. in Finnland und in Belgien) Ausweisdokumente angeboten. Um sicherzustellen, dass das Auslesen der Daten von Nutzern nicht ohne deren Wissen erfolgt, ist die Eingabe einer PIN nötig (z. B. in Großbritannien und in Spanien). Diese wird von einer Softwarekomponente angefordert, die auf einem mit dem Kartenlesegerät verbundenen Rechner installiert ist. Die Notwendigkeit der Zustimmung von Bürgern für das Auslesen ihrer Daten schützt die Privatsphäre und trägt zur Steigerung der Datensicherheit bei. Die Kontrolle der Bürger über die Daten auf dem neuen Personalausweis scheint, laut Ländervergleich, zu größerer Bereitschaft beizutragen, die Technologie zu benutzen. Die Anwendungssoftware (AusweisApp in Deutschland) sowie die Hardwarekomponente (Kartenlesegerät) sorgen dafür, dass der Ausweisinhaber entscheidet, ob, wann und wem er seine Daten elektronisch übermittelt.

Betrachtet man die Software getrennt von der Hardware, zeigen sich mehrere Aspekte als ausschlaggebend für die Sicherheit der neuen Personalausweise. Dabei geht es um die Zuverlässigkeit beauftragter Unternehmen, die Sicherheit der Speicherung und Aufbewahrung der Daten, die Sicherheit bei deren Transport und Verwendung sowie der Ausschluss einer Wiederverwendung der Daten ohne Zustimmung.

Für die Entwicklung und den Support der Anwendungssoftware wird die Verwaltung externe Partner beauftragen. Die Wahl des damit beauftragten Unternehmens hat große Bedeutung für die Sicherheit der Software und ihrer Pflege. Dies beeinflusst die Meinungsbildung der Nutzer über den gesamten Prozess der Verwendung eines elektronischen Identitätsnachweises. Daraus kann man schließen, dass nicht nur die Qualität der Software, sondern auch die Meinung über den Auftragnehmer die Nutzungsbereitschaft der Bürger beeinträchtigt.

Die Anzahl der Unternehmen, die für die Entwicklung einer solch umfangreichen und wichtigen Softwarekomponente die nötigen finanziellen Mittel, Personal und Erfahrung haben, ist gering. Unter anderem wurden in anderen EU-Ländern Microsoft, SAP oder Oracle und in Deutschland Siemens damit beauftragt.

Die obige Betrachtung der fünf Länder zeigt, dass nicht alle Staaten biometrische Daten verpflichtend aufnehmen. Weiterhin gibt es nicht in allen EU-Staaten nationale zentrale Datenbanken. Wenn es keine zentrale Datenbank gibt, existiert auch nicht die Gefahr, dass diese angegriffen wird. Jedoch bringt eine solche Informationsaufbewahrung Vorteile für die nationale Sicherheit, zum Beispiel bei der Lösung von Kriminalfällen mithilfe von Fingerabdrücken mit sich.

Großbritannien, Spanien und Österreich sind Länder, in denen die für den Personalausweis aufgenommenen Daten der Bürger größtenteils zentral gespeichert werden. Während in Großbritannien dies von der jetzigen Regierung als Risiko gesehen wird und eine Abschaffung des NIR geplant ist, haben Spanien und Österreich große Erfolge im Bereich der elektronischen Identität aufzuweisen. Österreich erhielt im Jahr 2005 eine Auszeichnung für das erreichte Datenschutzniveau. Der komplexe Prozess der Datenverschlüsselung und die Zuverlässigkeit der Algorithmen sorgen für die Sicherheit der zentralen Datenbank im Fall eines Angriffs. In Spanien wird eine strenge Kontrolle über die Zugriffe auf die Datenbank durchgeführt, indem man alle Zugriffe zurückverfolgt. Beide Verfahren steigern sowohl die objektive als auch die subjektive, von den Bürgern empfundene, Sicherheit.

Ein weiterer wichtiger Punkt ist das Risiko, dass die Daten der Bürger nach der Nutzung der Dienstleistung nicht von der Datenbank der Anbieter gelöscht werden. Die Gefahr einer Weiterverwendung darf nicht vernachlässigt werden. Des Weiteren ist der Staat für den Schutz der in der nationalen Datenbank und auf dem Chip des Personalausweises gespeicherten Informationen zuständig. Jedoch bleiben Datenbanken von Dienstleistungsanbietern angreifbar. Aus diesem Grund ist es sinnvoll, bei einem Identitätsnachweis im Rahmen des E-Commerce nur die notwendigen Nutzerdaten zu versenden. Verwaltungen können diesen Prozess regulieren, indem vorbestimmt wird, welche Daten für welche Anwendungen abgefragt werden dürfen. Weiterhin kann die Sicherheit der Daten durch die Verwendung eines Pseudonyms gestärkt werden. Mithilfe eines Clients (z. B. AusweisApp) wählt der Nutzer aus, welche Daten er freigeben möchte. Somit spielt die auf dem privaten Rechner installierte Software eine große Rolle bei der Auswahl der zu versendenden Daten.

Eine Schwachstelle bei der Nutzung elektronischer Dienstleistungen ist der Transport der Daten. Sowohl die Verwendung der auf dem Chip gespeicherten Daten als auch die Nutzung der zentral in der nationalen Datenbank aufbewahrten Daten ist mit einem Transport über das Internet verbunden. Es muss sichergestellt werden, dass der Bürger tatsächlich das unterzeichnet, was auf seinem Bildschirm erscheint, und dass seine Daten (u. a. auch die Signatur) während des Transports unverändert bleiben. Dafür sorgt EU-weit die Verwendung von Zertifikaten und kryptografischen Verfahren. Eine Sicherheitslücke in der Anwendungssoftware könnte allerdings den gesamten Prozess kompromittieren.

Zusammenfassung

In diesem Kapitel wurden bereits bestehende eID Projekte in anderen EU-Ländern charakterisiert. Dafür wurden die jeweiligen Rahmenbedingungen, rechtliche Vorschriften, Datenerfassungsanforderungen und Verwendungsmöglichkeiten berücksichtigt. Dies ergibt umfassende Informationen über die EU-weiten Erfahrungen mit der eID-Funktion der Personalausweise. Die Erfahrung der betrachteten Länder lehrt, dass die eID-Funktion des nPA vielversprechend ist. Wenn die wichtigsten Anforderungen berücksichtigt werden, ist die eID-Funktion attraktiv für Verwaltung, Bürger und Unternehmen.

4. Marktchancen für eID-Infrastrukturen in Deutschland

Innovationen sind die Treibkraft für Wachstum und Prosperität eines Unternehmens. Wichtig ist, dass die Neuartigkeit von Produkten bzw. Dienstleistungen nicht die entscheidende Rolle für den Erfolg hat. Große Bedeutung hat das durch die Marktsituation bestimmte Marktpotenzial (Bullinger/Scheer 2006, 257). Eine keinesfalls kleinere Auswirkung auf die Zukunft der Innovation hat ihre Markteinführungsstrategie. Sie muss individuell auf das Produkt, Unternehmen und den Markt zugeschnitten sein, um als adäquat bezeichnet zu werden und in Richtung erfolgreiche Umsetzung zu führen. Die Wahl der Vorgehensweise bei der Markteinführung kann zur Ursache für einen großen Erfolg oder für Misserfolg werden (Herrmann/Huber 2009, 240f).

Für die Einführung des nPA kommt keine gewöhnliche Markteinführungsstrategie infrage. Bei E-Government Projekten werden zwar elektronische Dienstleistungen behandelt, wie zum Beispiel bei E-Commerce, jedoch werden sie nicht von Unternehmen angeboten, sondern von Verwaltungen. Wichtig ist dabei, dass auf Verwaltungstätigkeiten nicht die bekannten Marktmechanismen wirken und keine Kunden per se existieren (Penski 1999, 94). Des Weiteren befriedigt der Bürger nach Ansicht Penskis nicht seine Bedürfnisse, sondern ist Träger von staatlichen Vorhaben und Anspruchsträger sowie Träger von Verpflichtungen. Darüber hinaus entstehen Netzeffekte erst dann, wenn viele Nutzer und Anbieter auf dem Markt für Online-Dienstleistungen vertreten sind. Aus diesen Besonderheiten ergibt sich, dass bei der Markteinführung von eID-Infrastrukturen nicht die gewöhnlichen Marktstrategien betrachten werden können.

4.1. Vorgehen zur Ermittlung von Marktchancen

Im folgenden Kapitel wird eine ausführliche Marktanalyse für den nPA durchgeführt. Zunächst wird sich mit den involvierten Marktakteuren auseinandergesetzt. Die Erkenntnisse aus dieser Untersuchung stellen die Basis für die Marktcharakteristika der eID-Infrastruktur in Deutschland dar. Nach Erläuterung der Strategieoptionen bei der Einführung von eID-Infrastrukturen, werden eID-basierte Geschäftsmodelle erläutert. Nachfolgend wird auf Anwendungsszenarien näher eingegangen. Im Anschluss werden Folgerungen über die Akzeptanz der eID-Infrastrukturen in Deutschland gezogen.

4.2. Marktanalyse für die Einführung des nPA in Deutschland

Die Analyse des Marktpotenzials basiert auf Betrachtungen des aktuellen Zustands des relevanten Marktes. Befasst man sich mit dem Marketing eines Anbieters, so muss man untersuchen, auf welchen Markt sich die Strategie und Aktivitäten beziehen sollen. Das Ergebnis dieser Untersuchung wird als Marktabgrenzung bezeichnet (Homburg/Krohmer 2009, 5). Die Marktabgrenzung ermöglicht eine

Marktanalyse, die drei Analysebereiche abdeckt – Akteure, Interaktionen zwischen den Akteuren und allgemeine Marktcharakteristika. Anschließend werden die Einführungsstrategien geschildert. Die Ergebnisse aus diesen Betrachtungen führen zu Erkenntnissen über das Marktpotenzial des nPA.

Vor der Durchführung einer Marktanalyse über den nPA sollten die einzelnen Märkte seiner Komponenten getrennt definiert werden. Der Markt für den nPA umfasst vier Teilmärkte (vgl. Abbildung 11).

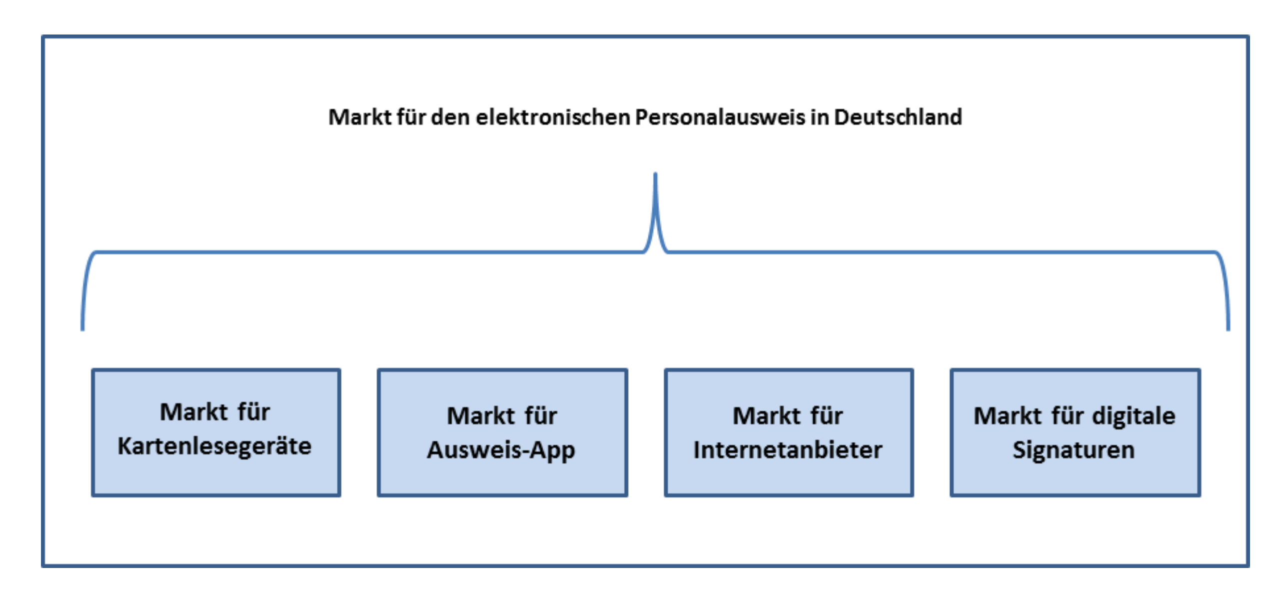


Abbildung 11: Markt für den neuen Personalausweis in Deutschland

Die unterschiedlichen Marktsegmente können wie folgt definiert werden:

(1) Markt für Kartenlesegeräte: Das Kartenlesegerät ist eine notwendige Komponente des nPA und ermöglicht die Identifikation mithilfe der Daten, die auf dem RFID-Chip des nPA gespeichert sind.

(2) Markt für die AusweisApp: Die AusweisApp ist die Authentifizierungssoftware, die es dem Kartenbesitzer erlaubt auf seinen Ausweis mittels seines PCs zuzugreifen und sich online zu authentifizieren. Die Software wird für Kartenbesitzer ohne zusätzliche Kosten verfügbar sein. Im November 2009 hat das Bundesministerium des Inneren (BMI) Siemens IT Solutions and Services, die Bundesdruckerei und Open Limit mit der Entwicklung dieser Anwendungssoftware beauftragt.

(3) Markt für Internetanbieter: Es ist möglich diese Liste um den Markt für die Internetanbieter zu erweitern, da eine Internetverbindung auch eine Voraussetzung für die Online-Identifikation und Online-Transaktionen ist.

(4) Markt für digitale Signaturen: Falls es der Kartenbesitzer wünscht, kann eine qualifizierte elektronische Unterschrift auf dem nPA gespeichert werden. Die Kosten für die elektronische Signatur müssen jedoch vom Kartenbesitzer getragen werden.

Die oben aufgeführten Teilmärkte sind die Hauptteilmärkte und stützen sich auf die einzelnen Produktkomponenten des nPA. Die Marktanalyse könnte auch um Märkte für Dienstleistungen erweitert

werden. Wenn sich z. B. die Regierung dafür entscheiden würde, seine Helpdesk und Unterstützungsdienstleistungen auszulagern, sollte der Markt für solche Dienstleistungen auch analysiert werden. Im Kontext unseres Projekts konzentrieren wir uns hauptsächlich auf die Akzeptanz des nPA im Allgemeinen und werden deshalb die einzelnen Marktsegmente nicht im Detail analysieren.

4.2.1.Marktabgrenzung

Die Einordnung des E-Government-Marktes als elektronischer Informationsmarkt wird als Grundlage für die konkrete Abgrenzung des Marktes für den nPA genommen. Eine Marktabgrenzung im Allgemeinen erfolgt über Objektkategorien wie Nachfrager, Anbieter, Produkte und Bedürfnisse (Homburg/Krohmer 2009, 5) und liefert Informationen, die wichtig für die Ermittlung der Marktchancen eines Produktes sind.

Bei E-Government-Projekten werden zwar elektronische Dienstleistungen behandelt, jedoch werden sie nicht von Unternehmen angeboten, sondern von Verwaltungen. Wichtig dabei ist, dass Verwaltungen nicht wie Unternehmen auf freien Märkten agieren. Auf Verwaltungstätigkeiten wirken nicht die privatwirtschaftlichen Marktmechanismen und es existieren keine Kunden per se. Bürger befriedigen nicht ihre Bedürfnisse, sondern sind Träger von staatlichen Vorhaben und Anspruchsträger sowie Träger von Verpflichtungen (Penski 1999, 94). Aus diesem Grund wird zwischen Bürgern und Konsumenten unterschieden. Bei der Nutzung von Dienstleistungen im Verwaltungsbereich spricht man von Bürgern. Wenn es dagegen um die Inanspruchnahme von Dienstleistungen in der Wirtschaft geht, spricht man von Konsumenten. Bei der Analyse der Marktchancen des nPA treten Nutzer sowohl als Bürger als auch als Konsumenten auf.

Ein weiterer wichtiger Aspekt bei der Marktabgrenzung ist die digitale Spaltung. Unter digitaler Spaltung wird das unterschiedliche Teilhaben von Bürgern an der Informationsgesellschaft verstanden, wodurch eine Aufteilung der Gesellschaft in Internet-Nutzer und Nicht-Nutzer entsteht (Scholz 2004, 285). Offliner haben nicht die Möglichkeit die eID-Funktion des nPA und die qualifizierte elektronische Signatur zu nutzen, aber auch nicht alle Bürger die über Internetzugang verfügen werden diese Funktionen des nPA verwenden. Seit Ende 2010 werden in Deutschland nur neue Personalausweise ausgestellt. Somit sind alle deutschen Staatsangehörigen verpflichtet, ihre auslaufenden Personalausweise durch den nPA zu ersetzen. Allerdings entscheiden Bürger selbst, ob sie über die Lichtbildidentifikation hinaus den nPA nutzen wollen. Laut Expertenschätzungen haben lediglich 30 % der Bürger die eID-Funktion des nPA freigeschalten. In diesem Beitrag werden nur deutsche Bürger betrachtet, die einen nPA besitzen und die die eID-Funktion und die qualifizierte elektronische Signatur verwenden.

Als Nächstes ist die kritische Rolle des Identitätsnachweises im Internet bei der Entwicklung von E-Business und E-Government zu berücksichtigen. Die Zuverlässigkeit von elektronischen Identitäts-

nachweisen sowohl seitens der Käufer als auch seitens der Anbieter gewinnt ständig an Bedeutung. Das stellt ein großes Potenzial für die Verwendung der eID-Funktion des nPA im E-Business dar. Dadurch werden nicht nur bestehende Online-Dienstleistungen vertrauenswürdiger gestaltet, es werden auch viele neue Anwendungen erst möglich. Dienste, die bis jetzt nicht realisierbar waren, da sie eine höhere Sicherheit voraussetzten oder rechtlich eine Identifizierung per Ausweis erforderten, werden mit der Einführung des nPA möglich. Es wird deswegen erwartet, dass die Anzahl der Unternehmen, die von der eID-Funktion Gebrauch machen werden, in naher Zukunft rapide steigen wird. Somit werden diese Unternehmen weitere Anbieter auf diesem Markt. Je mehr Anbieter und Nachfrager existieren, desto besser können Netzeffekte und die damit verbundenen Vorteile genutzt werden.

Aus diesen Erkenntnissen kann man die Schlussfolgerung ziehen, dass die Treibkraft für die Vermarktung von ID-Infrastrukturen an erster Stelle Verwaltungen sind, aber der langfristige Erfolg sich erst einstellt, wenn der private Sektor involviert wird, weil Nutzer dann mehr Verwendung für die eID-Funktion haben werden (Valkenburg et al. 2010, 4).

Zusammengefasst ergibt die Marktabgrenzung, dass ein größerer Markt für den nPA in Deutschland in Zukunft erzielt werden kann. Obwohl alle deutschen Bürger Zielgruppe bei der Verbreitung des nPA sind, kann heutzutage wegen der digitalen Spaltung ein Teil davon nicht als Nutzer gewonnen werden. Unternehmen und Verwaltungen bieten den Bürgern bereits einige Dienstleistungen an, aber eine Angebotserweiterung wird eine höhere Akzeptanz des nPA mit sich bringen. Experten erwarten, dass in Zukunft mehrere Anwendungen von den Wirtschaftsakteuren angeboten werden (Valkenburg et al. 2010, 4). Dadurch wird die Anzahl der möglichen Verwendungsgründe steigen, was mit einer Erhöhung der Nachfrage, des Angebots und der Produktauswahl assoziiert wird. Insgesamt lässt sich dadurch der für den nPA relevante Markt erweitern.

4.2.2. Akteure

Bei E-Government Projekten sind verschiedene Akteure involviert und betroffen. Als Grundlage für die Betrachtung der Akteure werden die Rollen der Beteiligten nach (Homburg/Krohmer 2009, 461f) herangezogen und um weitere involvierte Teilnehmer erweitert: Anbieter, Nutzer, Partner, Forschungsakteure, Intermediäre, Verwaltung und Wettbewerber. Die genannten Akteure werden im Folgenden näher erläutert.

4.2.2.1. *Anbieter*

Die Einführung des neuen Personalausweises soll die Nutzung der dafür entwickelten elektronischen Dienstleistungen ermöglichen und vorantreiben. In diesem Sinne werden die Rollen der Anbieter und der Nutzer festgelegt. Wer genau diese Rollen übernimmt, hängt von der Dienstleistung ab. Anbieter

können Verwaltungen, Behörden oder öffentliche Einrichtungen sein. Allerdings können auch Unternehmen elektronische Dienstleistungen anbieten, für deren Inanspruchnahme der nPA verwendet wird. Für beide Anbietergruppen lassen sich die dadurch entstehenden Vorteile ableiten. Die Potenziale, die die Anbieter anlocken sind Kostensenkung, Bürokratiekostenentlastung und Vereinfachungen bei der Erfüllung der Identifizierungspflichten. Für Unternehmen werden durch das Angebot von elektronischen Dienstleistungen die Kosten gesenkt, indem die Kunden und Geschäftspartner zuverlässiger identifiziert werden. Die Bürokratiekostenentlastung bei Unternehmen und bei Behörden wird durch die Verbesserung der Abwicklung von elektronischen Geschäftsprozessen einerseits, und durch die Optimierung von Antragsprozessen andererseits, erfolgen. Weiterhin können Dienstleistungen, die bis jetzt aufgrund eines fehlenden elektronischen Identitätsnachweises nicht medienbruchfrei erfolgen konnten (wie zum Beispiel Altersverifikation bei Unternehmen), nun vollständig über das Internet ablaufen. Weiterhin ist für Behörden das Angebot von elektronischen Dienstleistungen damit verbunden, dass Bürger das Dienstleistungsangebot außerhalb der Öffnungszeiten, unabhängig von Wartezeiten und ggf. unabhängig von Behinderungen nutzen können. Somit wird ein neues Potenzial zur Modernisierung und Bürgerfreundlichkeit entfaltet.

4.2.2.2. *Nutzer*

Die Segmentierung der Nutzer stellt das Fundament für die Marktanalyse dar. E-Government Dienstleistungen dienen v. a. den folgenden Kundengruppen: Bürgern, Unternehmen, Behörden und Staatsangestellten. Eine verfeinerte Segmentierung der natürlichen Personen findet man in (Turner et al. 2005, 441ff). Dieser Vorschlag wird in Tabelle 7 zusammengefasst.

Konsument	Konsumenten sind diejenigen Personen, die Güter von staatlichen Stellen erwerben, wie zum Beispiel Dienstprogramme oder Lottoscheine.
Klient	Klienten sind diejenigen Personen, die professionelle Dienstleistungen der Behörden regelmäßig über längere Zeit in Anspruch nehmen, zum Beispiel Gesundheitsleistungen und Bildung.
Bürger	Bürger sind diejenigen Personen, die Dienstleistungen der Verwaltung im breiteren Sinne benutzen, zum Beispiel Infrastrukturen wie Abwassersysteme und Autobahnen.
Subjekt	Subjekte sind diejenigen Personen, die gesetzlich verpflichtende Dienstleistungen der Verwaltung in Anspruch nehmen, ohne eine Alternative zu haben, wie zum Beispiel Steuerzahlung und Ausweispflicht.

Tabelle 7: Segmentierung der Bürger (Quelle: In Anlehnung an (Turner et al. 2005, 443)

Diese Segmentierung ermöglicht eine konkretere Betrachtung der Nachfrager von E-Government Dienstleistungen, obwohl die Kundengruppe Bürger sehr heterogen ist. Jeder Staatsangehörige handelt in jeder der vier Rollen – Konsument, Klient, Bürger, Subjekt. Die Zugehörigkeit zu einer der vier Gruppen wird durch Untersuchung der Dienstleistung bestimmt (Mintzberg 1996, 77). Bürger sind Träger staatlicher Vorschriften und Verpflichtungen, u. a. müssen sie der Ausweispflicht nachkommen und über einen nPA verfügen. In diesem Sinne sind sie als Subjekte zu betrachten. Wenn sie die AusweisApp von den Internetseiten der Verwaltung herunterladen, handeln sie als Konsumenten. Im Zusammenhang mit der Nutzung der eID-Infrastruktur gehören sie der Gruppe der Bürger an. Weiterhin werden den nPA-Inhabern elektronisch abwickelbare Verwaltungsdienstleistungen angeboten, deren Nutzer Klienten genannt werden. Da nach Homburg (2009, 464) eine Segmentierung Anforderungen nach Trennschärfe und zeitlicher Stabilität erfüllen soll, ist diese Unterteilung keine Segmentierung per se. Somit erweist sich nur die erste Ebene der Segmentierung als sinnvoll – Bürger, Unternehmen, Behörden und Staatsangestellte. Aufgrund der speziellen Eigenschaften des nPA kooperieren Staatsangestellte und Behörden, indem sie die Abwicklung verwaltungsinterner Abläufe unterstützen und werden nicht in der Analyse der Nutzer behandelt. Somit werden Nutzer von E-Government-Dienstleistungen in zwei Gruppen unterteilt – Bürger und Unternehmen. Weiter sind die elektronischen Dienstleistungsangebote von Unternehmen nicht zu vernachlässigen, für deren Inanspruchnahme die Verwendung der eID-Funktion des nPA notwendig ist. In diesem Sinne handeln natürliche Personen sowie wirtschaftliche Kunden als Konsumenten. Dabei ist zu vermerken, dass Unternehmen keine elektronische Identität haben. Um geschäftliche Tätigkeiten auszuüben, weisen sich Mitarbeiter der Unternehmen durch ihre elektronische Personalausweise aus.

Wichtig für die Analyse der Nachfrager ist die Untersuchung des Nutzungsaspekts – ob sie die Möglichkeit haben, den nPA zu nutzen, sowie ihre Bereitschaft, dies zu tun. Entscheidend ist der Zugang zu Rechnern mit Internet. Der Anteil der Haushalte mit Internetzugang lag 2008 bei 75 % man erwartet, dass dieser im Jahr 2012 bei etwa 87 % liegen wird (Bundesministerium für Wirtschaft und Technologie 2009, 63). Im Jahr 2010 wurden 72 % der Deutschen als Onliner bezeichnet, was mit drei Prozentpunkten mehr als im Jahr 2009 eine kleine Steigerung zeigt (o. V. 2010b, 10). Weitere 3,8 % sind Nutzungsplaner. Die restlichen 24,2 % der Bürger haben angegeben, sie wären Nichtnutzer ohne Beschaffungsabsicht (o. V. 2010b, 10). Die Anzahl der Unternehmen mit Internetzugang liegt bei 95 % in 2008 (Bundesministerium für Wirtschaft und Technologie 2009, 47). Aus dieser Betrachtung wird ersichtlich, dass zur Zeit die Anwendungsmöglichkeiten des nPA nicht alle potenziellen Nutzer ansprechen können. Diejenigen Bürger, die keinen Internetzugang besitzen, können die eID-Funktion des nPA nicht nutzen. Unternehmen ohne Internetzugang können sich nicht elektronisch authentifizieren um digitale Dienste von Verwaltungen oder anderen Unternehmen in Anspruch zu nehmen. Andererseits können Unternehmen ohne Internetanschluss keine elektronischen Dienstleistungen anbieten. Da nicht sichergestellt werden kann, dass alle Bürger und Unternehmen einen Internetzugang besitzen oder auch besitzen wollen, kann in naher Zukunft nicht auf die bisherigen Verwaltungstätigkeiten der

Behörden verzichtet werden. Denn auch Bürger, die über einen nPA verfügen, weichen nicht gänzlich auf die elektronischen Dienstleistungen aus. Gründe dafür sind die Gewohnheit, Angst vor neuen Technologien, aber auch fehlende Informiertheit über Dienstleistungsangebote. Das bekannteste Angebot ist die elektronische Steuererklärung (ELSTER), die 50 % der Deutschen kennen. Nur 31 % haben diese Leistung bis Juni 2010 benutzt. Die Reservierung eines Wunschkennzeichens wurde von 14 % in Anspruch genommen, obwohl etwa 25 % der Deutschen diese elektronische Dienstleistung kennen. Die Behördendienstportale sind den Nutzern kaum bekannt – nur 5 % der Deutschen kennen das zentrale Bürgerportal www.d115.de (o. V. 2010b, 2). Im Gegensatz zu den Planungen der Behörden - Einsparung von Mitteln bei klassischen Verfahren – führt dies einerseits zu möglichen Doppelbelastungen, da sowohl das klassische Verfahren weiterbetrieben, als auch das neue elektronische Verfahren betrieben werden muss, und andererseits zur unvollständigen Entfaltung des Potenzials der neuen Technologie.

4.2.2.3. *Partner*

Behörden in Deutschland sind eng miteinander verbunden (Scheer et al. 2003, 75). Die Abwicklung von Verwaltungsprozessen benötigt in 42 % der Fälle eine Kommunikation mit Behörden der gleichen staatlichen Ebene und in 23 % bzw. 15 % der Fälle die Zusammenarbeit mit Behörden einer unter- bzw. übergeordneten staatlichen Ebene (Scheer et al. 2003, 75). Aufgrund der Entwicklungen im IKT-Bereich können diese Prozesse verbessert werden, was mit strategischen, technischen und organisatorischen Aspekten verbunden ist. Für den Einsatz sowie für die Verwendung neuer elektronischer Infrastrukturen ist eine Zusammenarbeit der Verwaltungen unerlässlich (Scheer et al. 2003, 75). Betrachtet man Prozesse, die die Kooperation mehrerer Behörden veranlassen, spricht man von behörden- oder auch verwaltungsinternen Prozessen. In diesem Sinne sind Verwaltungen untereinander verwaltungsinterne Partner.

Allerdings laufen nicht alle Prozesse nur zwischen Verwaltungen ab. Die Verwaltung hat kein technisches Know-how, weswegen Unternehmen die Rolle des verwaltungsexternen Partners übernehmen und mit der Entwicklung von Software und Herstellung von Hardware beauftragt werden (Yildirim 2004, 210). In diesem Zusammenhang werden die verwaltungsexternen Partner auch Lieferanten genannt.

Verwaltungsexterne Partner spielen eine große Rolle bei der Entwicklung von E-Government-Angeboten (Yildirim 2004, 210). Es besteht die Möglichkeit, dass Unternehmen in Zukunft E-Government Projekte auch finanziell fördern. Für den neuen Personalausweis bedeutet dies, dass die Unterstützung durch Sponsoren u. a. dazu führen kann, dass neue Technologien eingesetzt werden können (Scheer et al. 2003, 75). Aufgrund der noch fehlenden finanziellen Mittel gilt zur Zeit für E-Government, dass teilweise noch veraltete Technologien eingesetzt werden (Scheer et al. 2003, 75).

Der Einsatz moderner und innovativer Technologien wird die Sicherheit und ggf. die Qualität der elektronischen Prozesse erhöhen. Somit haben Wirtschaftsakteure als verwaltungsexterne Partner eine große Bedeutung für E-Government Projekte.

4.2.2.4. *Forschungsakteure*

Der neue Personalausweis ist eine Innovation, bei der viele technische, organisatorische und rechtliche Aspekte zusammenspielen. Im Rahmen der Entwicklung des nPA wurde in engem Kontakt mit Forschungsakteuren zusammengearbeitet. Die Begleitforschung wurde in zwei Phasen aufgeteilt. Zunächst wurden Anforderungen an den Ausweis, seine Umsetzungs- und seine Nutzungsmöglichkeiten untersucht. Diese Phase wurde 2008 abgeschlossen. In der zweiten Phase wurden vier Studien von unabhängigen Fachleuten aus Wissenschaft und Forschung erstellt. Sie beschäftigten sich mit Haftungsfragen, mit der Entdeckung von technischen Risiken beim Einsatz des nPA auf dem Bürger-PC, mit der Akzeptanz in der Nutzung der AusweisApp und mit der kryptografischen Sicherheit der implementierten Verfahren. Die Ergebnisse beider Phasen hatten Auswirkungen auf den nPA und auf die AusweisApp (Bundesministerium des Inneren 2010a). Somit spielen Wissenschaftler, Universitäten und Forschungsinstitute eine wichtige Rolle im Projekt.

4.2.2.5. *Intermediäre*

Unternehmen unterstützen die Verwaltung nicht nur durch die Entwicklung von Komponenten, sondern auch durch die Abwicklung von Arbeitsprozessen, die bei jeder Kontaktaufnahme erfolgen. Ein Beispiel dafür ist die Überprüfung der Gültigkeit von Zertifikaten. In diesem Sinne wird manchen Privatunternehmen auch die Rolle der Intermediäre zugewiesen. Der nPA ermöglicht Bürgern die Nutzung von elektronischen Dienstleistungen der Behörden. Dafür müssen sich Bürger identifizieren, was mit Versand und Empfang von elektronischen Daten verbunden ist. Aufgrund des fehlenden technischen Know-hows kooperiert die Verwaltung bei der Einbindung der Informations- und Kommunikationstechnologie mit externen Stellen (Yildirim 2004, 210). Spezialisierte Privatunternehmen unterstützen Behörden, wenn elektronische Dienstleistungen angeboten werden sollen. Dies erfolgt durch die Übernahme von Funktionen, die vor jeder Kontaktaufnahme zwischen Bürger und Behörde notwendig sind, sowie auch durch die Abwicklung von Arbeitsprozessen, die unabhängig vom spezifischen Verwaltungsvorgang sind, wie zum Beispiel die Authentifizierung des Bürgers oder die Gültigkeitsprüfung von Zertifikaten (Yildirim 2004, 210f).

4.2.2.6. *Legislative*

Die Entscheidung über die Einführung des neuen Personalausweises in Deutschland wurde von der Legislative getroffen. Die Bundesregierung initiierte den Gesetzentwurf zur Einführung eines neuen

Personalausweises (Deutscher Bundestag o. J.). Die Legislative spielt nicht nur bei der Initiierung eine Rolle, sondern während das gesamte Lebenszyklus des nPA, darunter auch bei seiner Nutzung. Gesetze schaffen einen Bezugsrahmen für das Dienstleistungsangebot seitens Verwaltung und Unternehmen sowie für deren Inanspruchnahme durch die Bürger. So will der Staat mit dem neuen Personalausweis bestimmte Ziele erreichen. Als erstes Ziel wird die Einführung einer bundesweiten einheitlichen Infrastruktur für einen elektronischen Identitätsnachweis gegenüber der Wirtschaft bestimmt. Die Nutzung der biometrischen Merkmale soll die Zahl der Betrugsversuche senken. Auch der Sperrung von verlorenen oder gestohlenen Ausweisen dient dieser Zweck. Der Abgleich der biometrischen Merkmale sorgt für eine weitere Sicherheitsstufe, deren Umgehung sich als besonders schwierig gestaltet. Weiter soll durch die qualifizierte elektronische Signatur das identitätsrelevante Handeln im elektronischen Rechtsverkehr ermöglicht werden (Bundesregierung 2008). Daraus folgt, dass der Staat bestimmte Anforderungen und Rahmenbedingungen stellt. Wichtig hierfür sind die Sicherheit und Zuverlässigkeit des nPA und der QES sowie das Kennen von Rechten, Pflichten und Grenzen aller Beteiligten. Darüber hinaus werden Datenschutz und IT-Sicherheit gefördert und durch entsprechende Richtlinien geregelt.

4.2.2.7. *Wettbewerber*

In der Regel betrachtet man bei der Marktanalyse parallel zu den Kunden auch die Wettbewerber (Homburg/Krohmer 2009, 459). Hier ist anzumerken, dass es bei E-Government Projekten keine echten Wettbewerber gibt. Der nPA ist eine modernisierte Version des deutschen Personalausweises, deshalb existieren keine Konkurrenten bei der Ausstellung der Ausweise. Die für die qualifizierte elektronische Signatur notwendigen Zertifikate bekommt der Ausweisinhaber aber nicht vom Bürgeramt oder vom Bundesverwaltungsamt, sondern von einem privaten Signaturanbieter (Verbraucherzentrale Berlin 2010). In diesem Sinne gibt es Wettbewerb zwischen den Signaturanbietern. Betrachtet man die Anwendungen des nPA, herrschen Konkurrenz und Wettbewerb bei den öffentlichen Dienstleistungen. Wenn mehrere öffentliche oder private Unternehmen sich mit dem Entwurf einer öffentlichen Dienstleistung beschäftigen oder von der Verwaltung damit beauftragt wurden, konkurrieren sie untereinander (Klump 2006, 5). Im Falle des elektronischen Ausweises zum Beispiel wurden Siemens und Open Limit mit der Entwicklungsarbeit beauftragt. Weiter wird ein „virtueller“ Wettbewerb in den Behörden durch Leistungsvergleiche (Benchmarking) angestrebt bzw. die Verwaltung steht intern im Wettbewerb (Reichard 2003, 119ff). Auch bezüglich der Lesegeräte für den nPA gibt es Wettbewerb. Die Produkte mehrerer Kartenlesegerätehersteller wurden auf ihre Funktionstüchtigkeit im Zusammenhang mit dem nPA und der AusweisApp geprüft und stehen den Bürgern zur Auswahl (Bundesamt für Sicherheit in der Informationstechnik 2011c). Weiterhin betrachtet man die Forschung, die mit der Entwicklung eines innovativen Produktes, wie des nPA, verbunden ist. In diesem Zusammenhang spricht man über Wettbewerb in der Wissenschaft, der zwischen Universitäten, Instituten oder Wis-

senschaftlern besteht (Klump 2006, 5). Keine dieser Konkurrenz- und Wettbewerbssituationen beeinflusst die Ausstellung des nPA. Deswegen werden diese auch nicht als Konkurrenzsituation für die Vermarktung des nPA aufgefasst. In diesem Zusammenhang stellen die Wettbewerber keine Akteure bei der Marktanalyse dar.

4.2.3.Interaktion zwischen den Akteuren

Der Fokus dieser Betrachtung liegt auf den Interaktionen zwischen den wesentlichen Akteuren. Zunächst wird veranschaulicht (vgl. z. B. Abbildung 12), wie die Prozesse zwischen Dienstleistungsanbieter und –nutzer erfolgen.

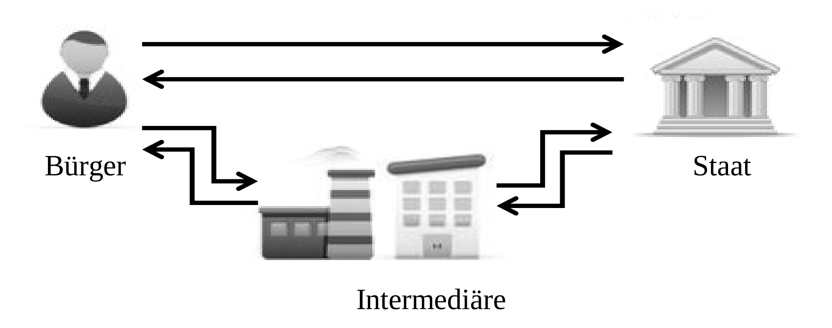


Abbildung 12: Interaktion zwischen Bürger, Staat und Intermediären (Quelle: Eigene Darstellung)

Wie bereits erwähnt, sind in einigen Fällen zwischen Staat und Bürger private Unternehmen als Intermediäre beteiligt. Dabei ist es möglich, dass in einem Prozess mehr als ein Intermediär involviert ist. Sobald der Bürger Kontakt mit der Behörde aufnimmt und eine Anfrage des Dienstes erstellt, fängt die Interaktion mit den Vermittlungsstellen an. Als Beispiel dafür werden die Beantragung des nPA und die gegenseitige Authentifizierung herangezogen.

Im Kontext der Beantragung eines nPA unterscheidet man drei Rollen – Behörden, Vermittlungsstellen und Ausweishersteller. Somit stellt sich der Prozess und der Datentransfer der Beantragung eines neuen Personalausweises als besonders komplex dar. Deswegen reicht es die Interaktion zwischen Behörde, Intermediäre und Ausweishersteller anhand des biometrischen Reisepasses zu erläutern. Bei Herstellung des nPA erfolgt die Speicherung biometrischer Merkmale auf dem Ausweis analog zum Reisepass. Anschließend erfolgt die Speicherung der elektronischer Identität, der Fingerabdrücke und der QES, worauf man im Kontext der Interaktion zwischen Akteure nicht näher eingehen muss.

Passbehörden sind die Stellen, bei denen Bürger den Reisepass und den nPA beantragen können. Der Antrag auf Verarbeitung biometrischer und persönlicher Daten wird an Vermittlungsstellen weitergeleitet, die zum Beispiel in Rechenzentren lokalisiert sind. Sodann werden die Produktionsdaten für den Ausweis dem Passhersteller übermittelt, der diese produziert und Rückmeldung an die Vermittlungsstellen und Passbehörden gibt (Bundesamt für Sicherheit in der Informationstechnik 2010, 4f). Für die

Datenübermittlung und Rückantworten wird der OSCI-Transport benutzt. Passbehörden, die dieses Verfahren nicht unterstützen können, wird eine Alternative auf der Basis von XML und WSDL/SOAP angeboten. Betrachtet man den OSCI-Transport von Daten, so spricht man von OSCI-Client und OSCI-Intermediär.

Passbehörde, Vermittlungsstelle und Passhersteller verfügen über eindeutige Authentifizierungszertifikate und je ein OSCI-Container, der unterschiedliche kryptografische Behandlung der Nutz- (Verschlüsselung für den Intermediär im Datentransport) und Inhaltsdaten (Verschlüsselung für Kommunikationspartner) beinhaltet. In dem OSCI-Container können ggf. die Daten verschlüsselt werden, wenn sie zwischen OSCI-Client und OSCI-Intermediär ausgetauscht werden (Bundesamt für Sicherheit in der Informationstechnik 2010, 20). Für das oben schematisch dargestellte Beispiel ist der OSCI-Client bei der Passbehörde lokalisiert. Wäre er bei der Vermittlungsstelle, so wäre diese ihr eigener Intermediär (Bundesamt für Sicherheit in der Informationstechnik 2010, 4).

Die Zuverlässigkeit der gegenseitigen Authentifizierung (siehe Abbildung 13) ermöglicht die privatwirtschaftliche Nutzung des neuen Personalausweises durch Bürger im Kontakt mit Unternehmen, Behörden und öffentlichen Einrichtungen. So können zum Beispiel Alterskontrollen, Versandhandel und Verwaltung von Benutzerkonten auf Serviceportalen im Internet medienbruchfrei erfolgen. Elektronische Dienstleistungsangebote seitens der Verwaltung, wie zum Beispiel Adressanmeldung und Einkommensteuererklärung, hängen durchaus von der Möglichkeit zur gegenseitigen Authentifizierung ab (Bundesministerium des Inneren 2008, 12).

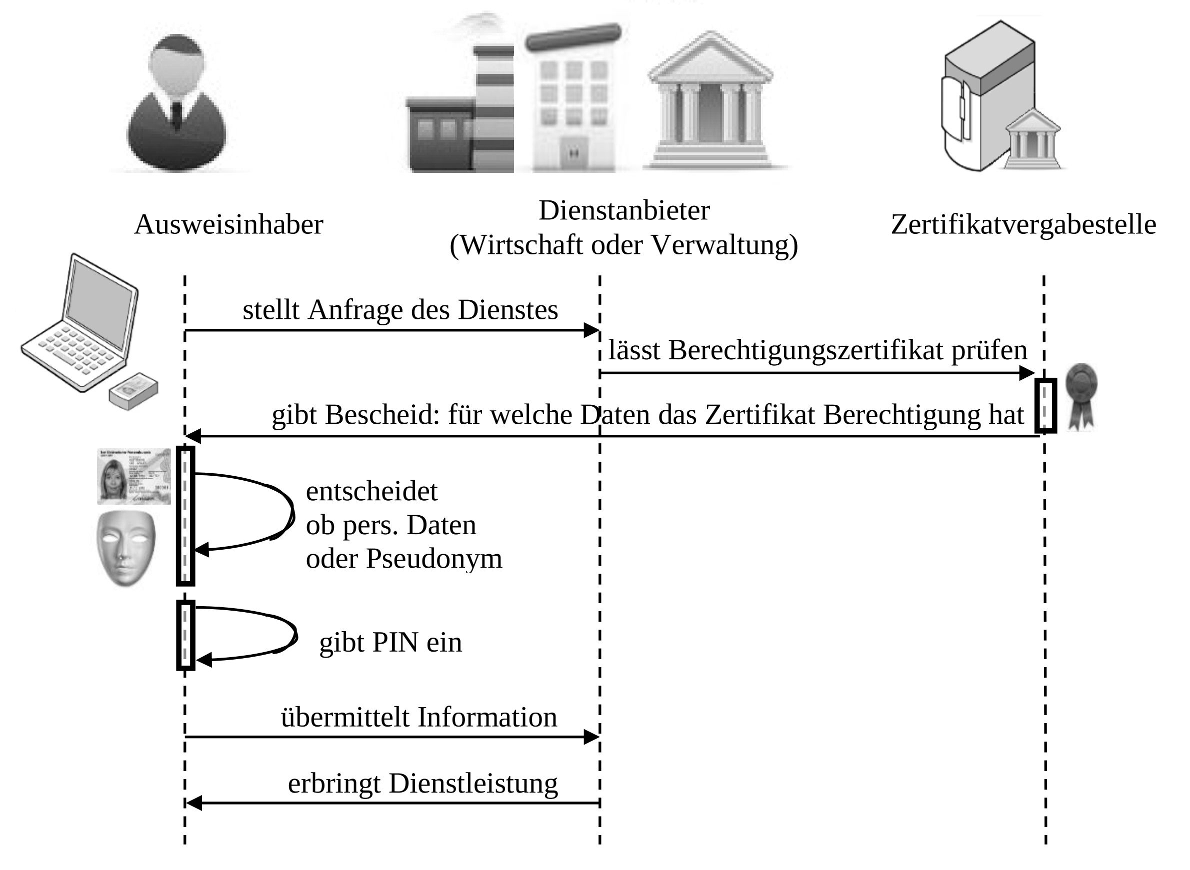


Abbildung 13: Gegenseitiges Authentifizieren (Quelle: Eigene Darstellung)

Weiterhin erleichtert der elektronische Identitätsnachweis auch die Kommunikation zwischen Unternehmen und Verwaltung (vgl. Abbildung 14). Unter anderem wird die Erfassung von Mitarbeiter, Kunden oder auch Geschäftsprozessen online-fähig (Bundesministerium des Inneren 2008, 50). Dadurch können an erster Stelle Steuer, Zugaben und Versicherungen der Angestellten ohne bürokratischen Aufwand erfolgen. Zweitens soll der nPA auch illegale Beschäftigungen und Schwarzarbeit verhindern, wie zum Beispiel bei Bauunternehmen und Gaststätten. Weiterer Schritt in dieser Richtung ist die Identitätskontrolle vor Ort bei diesen Unternehmen. Der nPA wird diese Kontrollen beschleunigen, indem über mobile Endgeräte mit Berechtigungszertifikaten und Kartenleserfunktion die Daten der Mitarbeiter ausgelesen und über Datenfunkverbindungen übermittelt werden (Bundesministerium des Inneren 2008, 50).

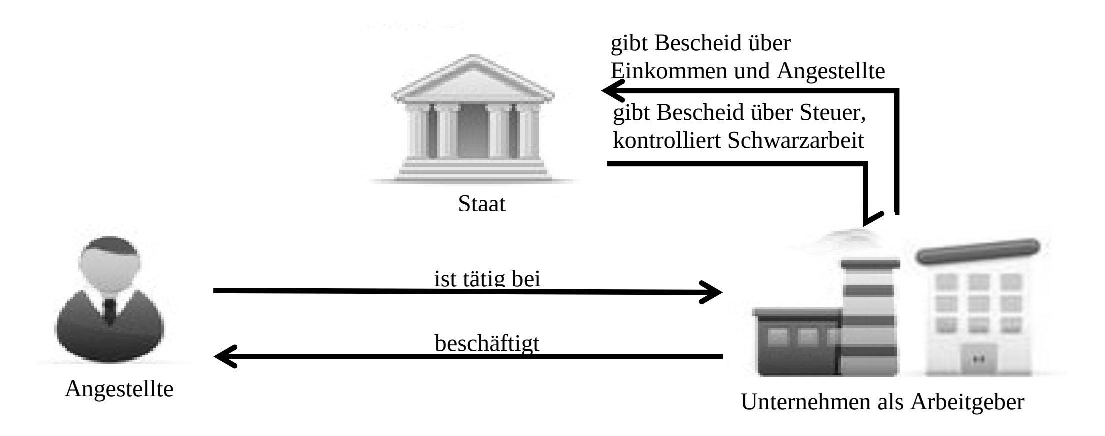


Abbildung 14: Interaktion zwischen Unternehmen, Angestellte und Staat (Quelle: Eigene Darstellung)

Abschließend wird die Interaktion zwischen Dienstanbieter, Verwaltung und Zertifikatvergabestelle behandelt (vgl. Abbildung 15). Um ein Zertifikat zu beantragen, muss der zukünftige Dienstleister erstmals Antrag an der Verwaltung stellen. Dieser wird dann geprüft. Falls der Dienstleistungsanbieter schon berechtigt ist, diese Daten zu erfragen, wird er an der Gebührenstelle weitergeschickt. Wenn nicht, dann muss ihm ein Zertifikat im Trust-Center ausgestellt werden.

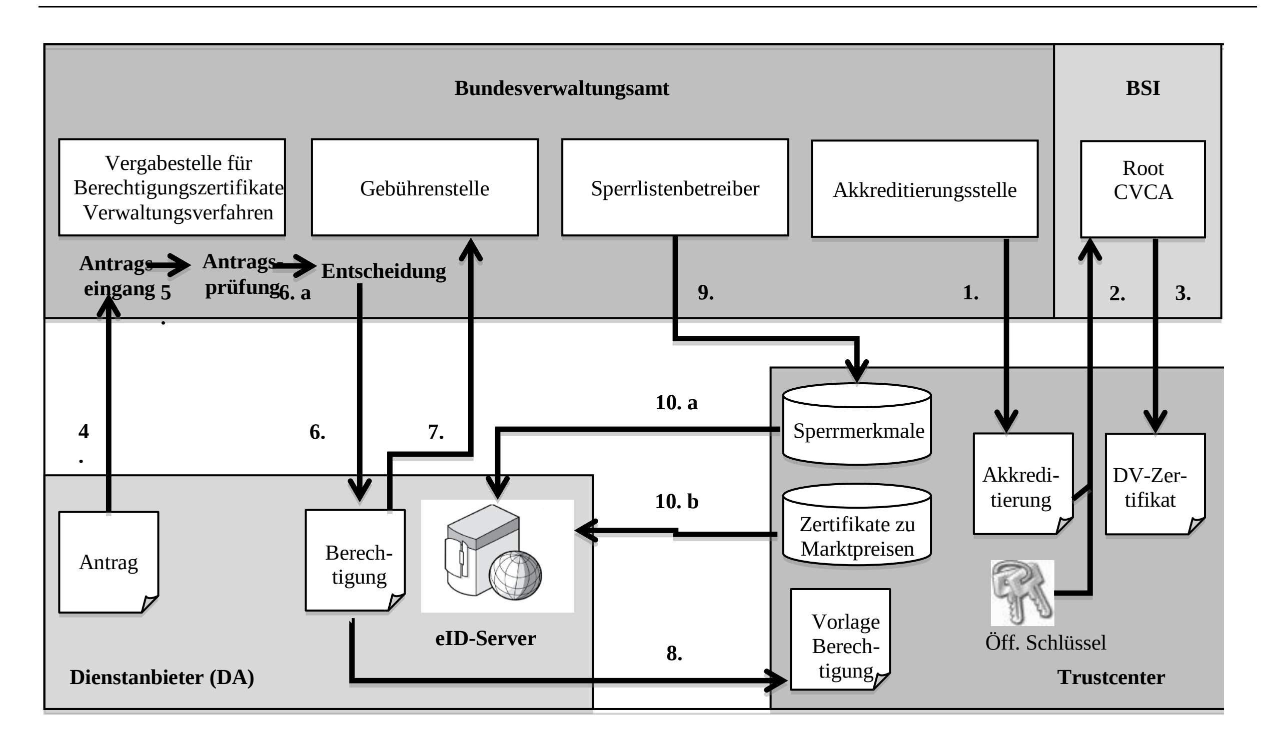


Abbildung 15: Interaktion zwischen Dienstanbieter, Verwaltung und Zertifikatvergabestelle (Quelle: Eigene Darstellung in Anlehnung an(Reisen 2009, 6)

4.3. Marktcharakteristika der eID-Infrastrukturen in Deutschland

Folgt man dem Leitfaden für Marktanalysen (Herrmann/Huber 2009, 240ff; Homburg/Krohmer 2009, 459), werden nach der Betrachtung der Akteure und deren Interaktionen die allgemeinen Marktcharakteristika untersucht. Man erläutert die kritischen Erfolgsfaktoren, die Markteintrittsbarrieren und abschließend das Timing und die Strategie der Markteinführung. Das Marktvolumen sollte auch hierfür beachtet werden. Da zum Zeitpunkt der Erstellung des Projektberichts jedoch keine Informationen über die Situation in Deutschland vorlagen, kann eine Abschätzung des Marktvolumens nicht stattfinden. Diese kann auch nicht anhand eines Ländervergleichs erfolgen, da zahlreiche Faktoren die Vermarktung in einem Land beeinflussen. Bei der Analyse der Eintrittsbarrieren, sowie bei der Betrachtung der Timingentscheidung und der Strategieoptionen bei der Markteinführung werden insbesondere auch Rückschlüsse über die passende Kommunikationsstrategie gezogen.

4.3.1. Eintrittsbarrieren

Wie bereits erwähnt, sind gewöhnliche Marktmechanismen auf E-Government-Projekte nicht anwendbar. Das gilt unter anderem auch bei den Eintrittsbarrieren. Die wesentlichen Markteintrittsbarrieren sind (1) Politik des Staates, (2) Umstellung der Kunden auf das neue Produkt, (3) Wettbewerber, (4) Kapitalerfordernisse, (5) Zugang zu wichtigen Vertriebskanälen (Herrmann/Huber 2009, 244ff).

4.3.1.1. *Politik des Staates*

Als wichtige Eintrittsbarriere betrachtet man üblicherweise die Politik des Staates. Dabei handelt es sich im Allgemeinen um Anforderungen und um Gesetze, die vor der Entwicklung des einzuführenden Produktes bereits verfasst wurden und auf die sich das Unternehmen bei der Entwicklung und Einführung des Produktes einzustellen hat. Im Gegensatz dazu behandelt man die Politik des Staates nicht als Eintrittsbarriere wenn es sich um E-Government-Projekte handelt. Der Staat ist der Initiator dieser Projekte. Damit befassen sich zunächst die Ministerpräsidentenkonferenz und die E-Government-Staatssekretäre (des Bundes und des Landes). Daraufhin werden die Ministerien mit der Vorbearbeitung des Projekts, dem Erproben und der Einführung des nPA beauftragt (Bundesregierung 2008). Insbesondere wurden im Falle des nPA die dafür relevanten Gesetze synchron zu seiner Entwicklung erlassen.

4.3.1.2. *Kundenumstellung*

Bei der Charakterisierung der möglichen Barrieren für die Markteinführung und den -eintritt, wird auch die Umstellung der Kunden auf das neue Produkt beachtet. Wie bereits erläutert, sind alle deutschen Bürger verpflichtet, nach Ablauf der Gültigkeit ihres alten Personalausweises, sich den nPA zu beschaffen. Da die Ausstattung mit neuen Personalausweisen sukzessive abläuft, wird eine Umstellung vom alten Personalausweis auf den neuen Personalausweis bis spätestens Ende 2020 abgeschlossen sein. Weitere Aspekte, die zu erschwerter Markteinführung führen können, werden im Folgenden behandelt.

4.3.1.3. *Kapitalerfordernis*

Bei der Einführung des neuen Personalausweises in Deutschland ist an verschiedenen Stellen zu investieren. Dabei lassen sich fünf Gruppen der wichtigsten Kapitalerfordernisse ableiten. Erstmals entstehen Kosten für die Entwicklung der AusweisApp. Die Entwicklung und der Support für die AusweisApp werden für drei Jahre vom Bundesinnenministerium finanziert. Es wird erwartet, dass sich der Markt danach für eID-Services in Deutschland so weit entwickelt haben wird, dass Anbieter mit eigener kommerzieller Zugangssoftware die Versorgung übernehmen werden (Borchers 2010a). Das Bundesministerium des Innern (BMI) hatte den Auftrag für die Erstellung der AusweisApp an die Firma Siemens IT Solutions and Services vergeben, welche als Generalunternehmen Open Limit mit der Softwareentwicklung beauftragte. Die Höhe dieser Investition seitens des Bundesinnenministeriums wird in der Literatur nicht genauer beziffert.

Neben der AusweisApp ist auch in einen eID-Server zu investieren. Dieser Teil der Software ist nicht kostenlos und soll über sogenannte eID-Hoster, für 2.750 Euro im Monat bei einer Einrichtungsgebühr

von 7.500 Euro, als Software-Service verkauft werden. Auch hier geht man beim Bundesinnenministerium davon aus, dass sich ein Markt entwickeln wird und deswegen die Preisfindung noch nicht abgeschlossen ist (Borchers 2010a).

Die dritte große Investition sind die 1.5 Millionen Sicherheitskits mit einem Wert von 24 Mio. Euro, die von Ende 2010 bis Ende 2011 an Bundesbürger verschenkt werden sollen, um die Akzeptanz des neuen Personalausweises zu fördern. Diese Summe wird im Rahmen des Konjunkturpakets II bereitgestellt. Die Sicherheitskits sollen nur Basis-Lesegeräte enthalten. Mit 7 Millionen Euro im Jahr 2010 steht die Werbung an der vierten Stelle bei den Kapitalerfordernissen. Diese Zahlen beziehen sich auf die deutschlandweite Einführung. Um die Aussage zu unterstützen, dass die IT-Projekte in E-Government nicht kurzfristig zu Gewinne führen, wird Peter Braun zitiert, Leiter des Einwohnermeldeamtes in Bochum: „Rund 765.000 Euro muss Bochum [...] zur Einführung ab November investieren, und an Einnahmen seien [...] 175.000 Euro zu erwarten“ (Vogt 2010).

Als Nächstes sind die Personalausweisbehörden im In- und Ausland mit der erforderlichen Hardware und Software auszustatten. Ab 2013 soll es möglich sein, den nPA bei Auslandsvertretungen zu beantragen (Bundesministerium des Inneren 2010e). Da dafür erhebliche Mittel notwendig sind, werden diese über ein Gebührenmodell finanziert, sodass keine zusätzlichen Belastungen für den Bundeshaushalt entstehen werden. Des Weiteren sind unter Umständen auch neue Personalausweisbehörden im Ausland einzurichten. Die Kosten, die bei diesem Schritt entstehen, sind in derzeit noch nicht bezifferbar (Bundesregierung 2008, 3).

Die fünfte Aufgabe, die zu erledigen ist, ist die Ausstattung der Zollfahndung, der mobilen Kontrollgruppen, des Grenzaufsichtsdienstes und der Dienststellen an den Drittlandsgrenzen mit der notwendigen Hardware (Lesegeräte). Im Gesetzentwurf für den nPA wurde dafür mit Kosten in Höhe von ca. 2.02 Mio. Euro gerechnet (Bundesregierung 2008, 4).

4.3.1.4. *Zugang zu Vertriebskanälen*

Zu einer gelungenen Bestimmung der Marketingstrategie gehört neben den benutzerorientierten Produkten auch die Auskunft von Vertriebskanälen. Die Nutzung des nPA wird den Bedarfsträgern einerseits als gewöhnlicher Lichtbildausweis ohne zusätzliche Funktionen, andererseits auch als elektronischer Identitätsnachweis über das Internet angeboten. Das heißt, dass zu den bereits vorhandenen persönlichen, schriftlichen und sprachtelefonischen Vertriebskanälen auch das Internet hinzugefügt wird. Es ist dabei zu beachten, dass dieser neue Vertriebskanal allerdings wegen der digitalen Spaltung nicht alle Nutzergruppen anspricht.

4.3.2.Timing der Markteinführung

Im Juli 2008 traf das Bundeskabinett in Berlin die Entscheidung, dass der neue Personalausweis im November 2010 für die deutschen Bürger erhältlich sein wird (Deutscher Bundestag o. J.). Diese Timingentscheidung sichert unter anderem, dass der nPA der erste Ausweis mit eID-Funktion auf dem deutschen Markt ist. Somit spricht man über einen Markteintritt als Pionier. Es handelt sich um einen Produktentwicklungspionier, seitens des Produktentwicklungstimings und um einen Markteintrittspionier, seitens des Markteintrittstimings. Diese Kombination ergibt nach Trommsdorff und Steinhoff die Bezeichnung „Innovationsleader". Die Timingstrategie Pionier bringt viele Vorteile aber auch Nachteile mit sich. Chancen der Pionierstrategie liegen bei der Etablierung eines Standards, längere Verweildauer auf dem Markt, Kostenvorteile, günstige Konkurrenzsituation auf dem Markt und Chancen bei der Preispolitik. Obwohl alle diese Kriterien im Allgemeinen tatsächlich als Vorteile betrachtet werden können, so ist das beim nPA jedoch nicht der Fall. Die Festlegung eines Standards, des Preises, der Kosten, des politischen Spielraums und der Verweildauer auf dem Markt werden von der Verwaltung selbst festgelegt und mithilfe der Gesetzgebung geregelt. Die Konkurrenzsituation wurde im Abschnitt 4.3.1 von der gewöhnlichen Situation des Wettbewerbs abgegrenzt. Auch bei den Markteintrittsbarrieren wird ein Sonderfall bezüglich des nPA betrachtet (vgl. Abschnitt 4.3.1). Der einzige Pluspunkt aus der Liste von Trommsdorff und Steinhoff, der auf den nPA übertragen werden kann, ist somit der Imagevorteil. Die Erläuterung der Risiken, mit denen bei der Pionierstrategie gerechnet wird, wird mit der Imagefrage eingeleitet. Allerdings geht es hier um Imageverlust durch unausgereifte Produkte. Ohne Annahme dieses Risikos können jedoch keine Innovationen auf den Markt gebracht werden. Die Neuartigkeit von Produkten ist mit weiteren Nachteilen für den Pionier verbunden – die Kosten und der Aufwand. Darunter werden die Kosten und der Zeitaufwand für die Forschung und für die Entwicklung subsumiert. Auch die Sammlung von Informationen über Markt- und Technologieentwicklungen ist mühsam für den Pionier. Das größte Risiko ist aber der Kunde selbst. Als Pionier muss man mit großem Überzeugungsaufwand rechnen. Beim nPA u. a. auch deshalb, da es zwar verpflichtend für die Bürger ist über den Personalausweis zu verfügen, die Nutzung zu Zwecken der E-Government-Dienstleistungen aber freiwillig bleibt. Kosten und Zeitaufwand für Forschung und Entwicklung dieser Infrastruktur sind hoch, aber sie waren von langer Hand für die Verwaltungsmodernisierung geplant, weswegen man sie beim nPA nicht als Nachteil betrachtet, sondern mehr als Notwendigkeit. Insgesamt ist der nPA mit Erwartungen für Gefahren, aber auch Erfolgen verbunden. Klaus König (1995, 349) warnt vor der Erweckung falscher Erwartungen beim Bürger, wenn im Allgemeinen von Dienstleistung und Kunde die Rede ist. Im Falle der Einführung einer innovativen Technologie, wie den Identitätsnachweis im Internet und das Angebot von mehreren elektronischen Dienstleistungen, sollte man von vornherein mit falschen Erwartungen beim Nachfrager, egal ob Bürger oder Unternehmen, rechnen. König ist entgegenzusetzen, dass durch dieses Leistungsangebot neue Umgangsformen entstehen, wie zum Beispiel, dass der Bürger als Kunde betrachtet wird. Somit wird

eine höhere Akzeptanz der Verwaltung erwartet. Beispiel dafür sind u. a. die zunehmenden Online-Angebote der Verwaltungen.

4.3.3. Strategieoptionen für die Markteinführung

Zunächst sollen in diesem Abschnitt die Einführungsstrategien im Rahmen des E-Government besprochen werden. Anschließend werden die Ziele analysiert, die mit der Einführung des nPA erreicht werden sollen. Zuletzt ist noch zu diskutieren, welche Leistungen bis zur Einführung des nPA zu erbringen waren.

Um gezielt eine Strategie verfolgen zu können, sind anfänglich die Ziele zu bestimmen, die durch die Entwicklung und Einführung des Projekts realisiert werden sollen (Scheer et al. 2003, 36). Beispiele von Zielen bei E-Government-Lösungen können u. a. die Steigerung der Effizienz, der Effektivität, der Qualität, der Flexibilität und der Kundenorientierung sein.

Nach Scheer, Kruppke und Heib (2003, 36f) ist es nicht sinnvoll, Strategien ohne Prozesse zu behandeln, da sie voneinander abhängig sind und sich gegenseitig beeinflussen. Die Realisierbarkeit der Strategie ist nur nach einer Rückkopplung mit den Prozessen abschätzbar. Sollte die Strategie nicht realisierbar sein, so wird sie geändert und die Prozesse werden von Neuem abgeleitet. Dieses Prinzip nennt man „Process follows strategy". Analog lässt sich idealerweise auch die Aufbauorganisation an der Strategie anpassen. Damit es zu einer tatsächlichen Umsetzung kommen kann, sollen Verwaltungsstrategie, -prozesse und -struktur langfristig miteinander harmonisieren. Externe Faktoren (Rahmenbedingungen), wie z. B. die Marktsituation, haben auch einen nicht vernachlässigbaren Einfluss. Diese Vorschriften werden in Abbildung 16 zusammengefasst und sollen bei allen E-Government Lösungen angewandt werden.

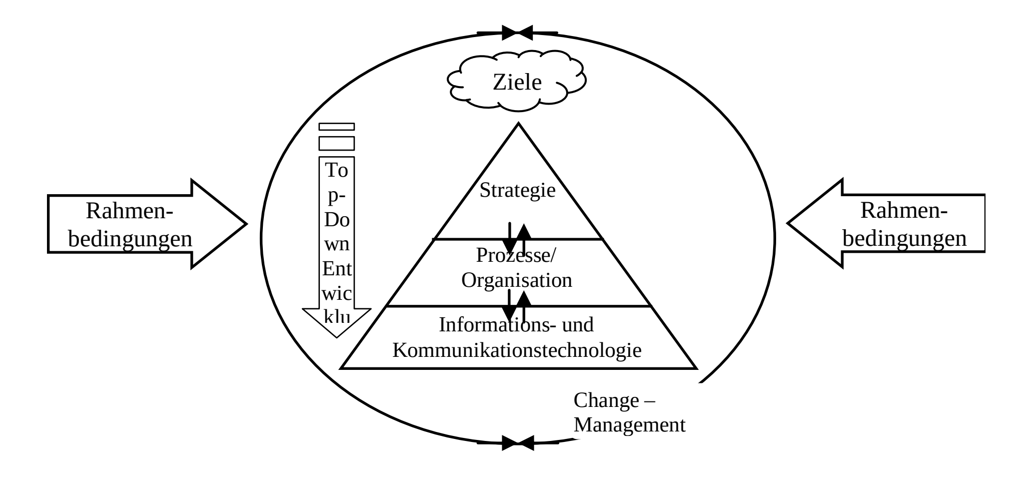


Abbildung 16: E-Government Lösung (In Anlehnung an Scheer/Kruppke/Heib 2003, 36)

Der Projektgruppe E-Government des BSI zufolge, verlangt der Weg zur Einführung einer E-Government-Dienstleistung in der Regel gravierende organisatorische Änderungen in den Geschäfts-

prozessen einer Behörde. Die Vertriebskanäle für die Dienstleistungen ändern sich und die manuelle und papiergebundene Abwicklung der Abläufe geht in eine elektronische Bearbeitung über, was „... eine völlige Umstrukturierung der verschiedenen Prozessketten ...”) erfordert. Bei E-Government handelt es sich nicht allein um Hard- und Software, sondern vielmehr um einen komplexen Prozess der „...tief greifenden organisatorischen Neuorientierung der Behörde als Ganzes ...“ (Bundesamt für Sicherheit in der Informationstechnik 2005, 4). Dies erfordert eine sorgfältige Planung und Systematik. Es wurde eine für E-Government-Projekte allgemeingültige Struktur angenommen, die das Gesamtprojekt in eine Folge überschaubarer Teilschritte untergliedert. So ergibt sich eine Abfolge von sechs Phasen: Initialisierung, Strategie, Analyse, Konzeption, Realisierung und Test, Einführung und Inbetriebnahme (Bundesamt für Sicherheit in der Informationstechnik 2005, 4). Im Folgenden wird die erste Aktivität der Phase 6 geschildert: „Festlegung der Einführungsstrategie“.

Der Leiter des E-Government Teams ist der Initiator bei Festlegung der Einführungsstrategie für jedes E-Government-Projekt. Für die Durchführung sind das E-Government Kernteam und die Behördenleitung zuständig, sowie auch Organisations- und Fachverantwortliche, die individuell für die Projekte bestimmt werden (Bundesamt für Sicherheit in der Informationstechnik 2005, 4). Man unterscheidet bei der Einführung zwischen zwei Vorgehensweisen. Zunächst gibt es die schrittweise Einführung, bei der man Etappen und die dazu passende Reihenfolge der Aktivitäten bestimmt. Weiter kann man die Anwendung auch sofort als Ganzes einführen, was man auch „Big-Bang“ Lösung nennt (Bundesamt für Sicherheit in der Informationstechnik 2005). Das ist auch die Vorgehensweise beim nPA. Seit Ende 2010 wird nicht mehr der klassische, sondern nur der neue Personalausweis ausgestellt. Dabei werden die Online-Dienstleistungen mit der Zeit eingefügt, was aber nicht mit einer schrittweisen Markteinführung zu verwechseln ist.

Der wesentliche Beitrag dieses Kapitels besteht darin, Aussagen über die Markteinführungsstrategien für den nPA herauszuarbeiten. Nach Erläuterung des dafür notwendigen Hintergrundwissens soll im Folgenden die Einführung des nPA näher betrachtet werden.

Im Grobkonzept für die Einführung des nPA in Deutschland wurden konkrete strategische Ziele für die Einführung abgeleitet, die als Leitlinien für die Ausgestaltung des nPA übernommen werden. Der neue Personalausweis ist in erster Linie ein Schritt in Richtung Verwaltungsmodernisierung. Die wichtigsten Eigenschaften, über die der nPA verfügen muss, sind Zuverlässigkeit, vielseitige Anwendungsmöglichkeiten und benutzerfreundliche Handhabung. Dafür sorgt die Erhaltung primärer Ziele für die Einführung, die nachfolgend erläutert werden sollen.

Weltweit wächst der Bedarf nach Sicherheit. Die Zuverlässigkeit eines Produkts ist eine seiner wichtigsten Eigenschaften. Für Identitätsnachweise ist es von größter Bedeutung, dass sie maximal sicher gegen Manipulationen sind. Für den neuen Personalausweis bedeutet dies, dass er nicht nur die Sicherheitsmerkmale eines Lichtbildausweises bewahren soll, sondern auch, dass seine elektronische

Nutzung einwandfrei und zuverlässig funktioniert. Somit ist die Sicherheit das führende Ziel für die Einführung. Im Grobkonzept für die Einführung des nPA in Deutschland wird dieses Ziel folgendermaßen formuliert: „Total- und Verfälschungen des Dokuments [sollen] soweit erschwert werden, dass diese – auch unter Einsatz moderner Technologien – nur mit kaum vertretbarem logistischen, technischen und finanziellen Aufwand vorgenommen werden könnten." (Bundesministerium des Inneren 2008, 43). Die Handlungen, die diesem Ziel dienen, sind die Aufnahme der biometrischen Merkmale in elektronischer Form (Fingerabdrücke [freiwillig] und Gesichtsbild) und die Verbesserung der Fälschungssicherheit durch die Verwendung kryptografischer Mechanismen (Bundesministerium des Inneren 2008, 43). Mindestsicherheitsstandards gibt es für den nPA in Deutschland nicht, da es sich um ein neuartiges Produkt handelt. Deswegen wird die Vorgehensweise auf der sukzessiven Einführung dieser Technik in den anderen EU-Mitgliedstaaten angepasst. Somit wird das hohe Sicherheitsniveau sowohl in der reellen, als auch in der elektronischen Welt als bedeutendstes Ziel bestimmt.

Als nächstes Ziel wird im Grobkonzept die Vielzahl der Anwendungen und Benutzungsmöglichkeiten bestimmt. Der nPA soll nicht nur für seine hoheitliche Funktion und für Dienstleistungen der Verwaltungen genutzt werden, sondern auch in der Wirtschaft. Ein solcher Identitätsnachweis soll die Geschäftsprozesse vertrauenswürdiger und effizienter machen. Fördernd werden hierfür innovative Dienstleistungen im E-Government und im E-Business bereitgestellt. Mit steigender Anzahl angebotener elektronischer Dienstleistungen seitens der Wirtschaft wird erwartet, dass die Bereitschaft zur Nutzung solcher Angebote seitens der Bürger steigen wird (Bundesministerium des Inneren 2008, 44). Von großer Bedeutung ist dabei, dass diese von Anfang an zuverlässig und sicher sind, um einen Imageverlust zu vermeiden.

Ein weiteres Ziel der Einführung des neuen Personalausweises ist die Harmonisierung aller neuer Personalausweise in der EU mittels einer Online-Authentifizierung. Einerseits ist dies eine Grundlage eines EU-weiten Standards für neue Personalausweise. Andererseits ist es wichtig, dass der Identitätsnachweis von deutschen Bürgern in anderen EU-Ländern reibungslos erfolgen kann et vice versa. Weiter ist die Ermöglichung eines sicheren grenzüberschreitenden elektronischen Geschäftsverkehrs wichtig (Bundesministerium des Inneren 2008, 44). Um das zu erreichen, muss man während des gesamten Projekts für die Entwicklung und die Einführung mit anderen EU-Ländern zusammenarbeiten.

Diese Ziele werden bei der Entwicklung und Einführung aller Anwendungsmöglichkeiten des nPA verfolgt. Sowohl im privatwirtschaftlichen Kontext, als auch für den Kontakt mit Behörden und Organisationen stehen oben genannte Ziele für jede einzelne Benutzungsmöglichkeit im Vordergrund. So wird, zum Beispiel, bei der Planung eines Umstiegs von der klassischen Adressanmeldung zur Online-Anmeldung mit folgenden Aktivitäten gerechnet. Nachdem der elektronische Identitätsnachweis erfolgt, wird dem Meldepflichtigen „ein weitgehend vorausgefülltes Meldeformular zur Verfügung gestellt" (Bundesministerium des Inneren 2008, 49). Gegebenenfalls kann eine elektronische Signatur erfolgen. Über eine gesicherte Verbindung werden die Daten an das Melderegister übermittelt. Das ist

nur eine Möglichkeit für die Nutzung des nPA im E-Government. Für die Benutzung vom nPA oder der elektronischen Signatur im E-Government und E-Business, sowie auch für die Automatisierung von Geschäftsprozessen, muss man jede mögliche Anwendung separat betrachten, um die konkreten Aktivitäten für die erfolgreiche Einführung bestimmen zu können. In diesem Beitrag wird nicht näher auf die zahlreichen Anwendungsmöglichkeiten und zugehörigen Aktivitäten eingegangen, da bei allen dieselben Ziele verfolgt werden, die gleichen Vertriebskanäle und Mittel für den Identitätsnachweis benutzt werden und die Ergebnisse aus dieser Betrachtung zum größten Teil analog zu dem Beispiel für die Adressanmeldung sind.

Die ersten Teile des Personalausweisgesetzes sind seit 01. Mai 2010 in Kraft getreten (Bundesministerium des Inneren 2010f, 9). Das ist eine wichtige Voraussetzung bei der Verfolgung des Ziels, um den nPA auch in der Wirtschaft zu benutzen, da somit seit Mai 2010 die Unternehmen an der Entwicklung solcher Dienste arbeiten können. Die genauere rechtlichen, technischen und organisatorischen Rahmenbedingungen, die den nPA betreffen, sind zum 04. Juni 2010 in Kraft getreten. Nach der Gebührenverordnung vom 09. Juli 2010 und dem Inkrafttreten der Verordnungen und des Gesetztes vom 01. November 2010 sind die rechtlichen Grundlagen bis auf Weiteres vollständig.

Mit der Herstellung des Personalausweises wurde die Bundesdruckerei beauftragt. Da die Produktion ein komplexer Prozess ist, musste eine Produktionsstrecke des Maschinenparks in der Bundesdruckerei aufgebaut und die Transportstrecke eröffnet werden. Der Termin dafür war der 01. Juli 2010. Somit können aus allen Personalausweisbehörden und Passbehörden Anträge für das neue Datenaustauschformat XHD gestellt werden (Bundesministerium des Inneren 2010f, 10). Der „flächendeckende Rollout der Hard- und Softwarekomponenten“ (Bundesministerium des Inneren 2010f, 10) wurde für den 19. Juli 2010 geplant. Mit der Produktionsanlage in Betrieb und der Freigabe des abschließenden Designs wird die Frage über den Stand der Produktion vollständig abgedeckt.

Kein Produkt von einer dermaßen großen Bedeutung kann ohne Testmaßnahmen freigegeben werden. Deshalb wurde ein Feldtest in 27 Behörden für den Zeitraum vom 02. Januar – 23. Juli 2010 geplant (Bundesministerium des Inneren 2010f, 11). Nachdem der Feldtest abgeschlossen wurde und dadurch Hinweise für den Rollout der finalen Komponenten gewonnen wurden, plante man „ab dem 15. August die Systeme in der Bundesdruckerei für alle 5.500 Personalausweisbehörden“ zu öffnen, „um die Möglichkeit zu geben, die Verfahren aus jeder Behörde im Land zu testen“ (Bundesministerium des Inneren 2010f, 11). Dadurch konnte festgestellt werden, welche Behörden für den 01. November 2010 bereit sind.

Aufgrund des Datenschutzes ist es besonders wichtig, den Stand der Vergabe von Berechtigungen zu verfolgen. Seit dem 01. Mai 2010 ist eine Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt eingerichtet (Bundesministerium des Inneren 2010f, 12). Das geplante Vorgehen bei der Vergabe von Berechtigungszertifikate sieht vor, dass die, für eine Anwendung erforderlichen, Daten

von vornherein festgelegt werden, sodass später keine zusätzlichen Daten rausgegeben werden müssen. Dieses Vorgehen wird „Entwicklung von Standardszenarien für die Verwendungspraxis" genannt und war zum 29. Juni 2010 „nahezu fertiggestellt" (Bundesministerium des Inneren 2010f, 12).

Um eine optimale Tätigkeit der Personalausweisbehörden zu sichern, muss als weiterer Schritt in der Einführung eine Schulung der Mitarbeiter eingeplant werden. Wegen des direkten Kontakts mit den Bürgern spielen diese Mitarbeiter eine große Rolle beim ersten Eindruck, den sich die Bürger über den nPA bilden werden. Die Fähigkeit kompetent auf- und erklären und über die Chancen und Risiken informieren zu können wird durch Qualifikation der Mitarbeiter erzielt. Nicht nur die Erklärung seitens der Mitarbeiter, sondern auch die Aufklärungsmaterialien, die den Bürgern angeboten werden, haben hierfür eine Bedeutung. Eine E-Learning Plattform soll den Lernprozess der Mitarbeiter erleichtern. Ihre Einführung wurde für August 2010 geplant. Dazu wurden Multiplikatoren aus allen Bundesländer geschult, die dann vor Ort die Mitarbeiter vorbereiteten (Bundesministerium des Inneren 2010f, 14).

Hauptvorteil des nPA gegenüber dem klassischen Personalausweis sind die elektronischen Anwendungen. Um die Dienste am 01. November 2010 im Netz zur Verfügung stellen zu können, wurden Anwendungstests benötigt.

Unter der Einführung des nPA versteht man die Markteinführung der gesamten ID-Infrastruktur. Die AusweisApp ist ein wichtiger Teil davon und wird seit 01. November 2010 angeboten. Bei der Softwareentwicklung arbeitete man parallel an einer Studie zur Benutzerfreundlichkeit, um Verbesserungen dieser einbeziehen zu können. Auch die eID-Services waren zum 01. November 2010 geplant. Am 29. Juni 2010 ging man davon aus, „dass mindestens zwei Unternehmen diesen als Dienstleistung am Markt anbieten werden" (Bundesministerium des Inneren 2010f, 17), die u. a. als eID Service Provider für kleinere und mittelständische Unternehmen gesehen werden.

Begleitend zu der Einführung wurden vier Studien in Auftrag gegeben. Sie beschäftigen sich „mit Haftungsfragen im Zusammenhang mit dem elektronischen Identitätsnachweis", mit „Restrisiken beim Einsatz des Bürgerclients auf dem Bürger PC", mit der „Akzeptanz in der Nutzung der AusweisApp und des Personalausweises" und „mit der kryptografischen Sicherheit der implementierten Verfahren" (Bundesministerium des Inneren 2010f, 17). Als letzte Maßnahme bei der Einführung betrachtet man die IT-Sicherheitskits. 24 Mio. Euro werden dabei für die Anschaffung von ungefähr 1,5 Mio. Lesegeräte ausgegeben, die den Bürgern kostenfrei zur Verfügung gestellt werden. Am 14./15. Juni 2010 wurde entschieden (Bundesministerium des Inneren 2010f, 9), dass man die Ausgabe von 1,46 Mio. IT-Sicherheitskits fördern wird (1,23 Mio. Basiskartenleser und 230.000 höherwertige Kartenleser). Dadurch soll die Onlinenutzung des nPA bei den Bürgern gefördert werden. Somit wurden die einzelnen Tätigkeiten bei der Einführung des nPA und deren, für den 01. November 2010 geplanten, Stand geschildert.

Zusammenfassung

Durch die Einführung des neuen Personalausweises auf dem deutschen Markt wird die vollständig elektronische Abwicklung von Prozessen ermöglicht. Die Zuverlässigkeit der eID-Funktion erlaubt deutschen Bürgern die Inanspruchnahme von Online-Dienstleistungen. Diese können sowohl von Verwaltungen als auch von privaten Unternehmen angeboten werden. Somit trägt der nPA einerseits zur Verwaltungsmodernisierung und andererseits zu einer einheitlichen staatlich geregelten Infrastruktur zum Identitätsnachweis bei Unternehmen bei. Es sind komplexe Beziehungen und Interaktionsmodelle entstanden, die viele Akteure involvieren. Zahlreiche Erfolgsfaktoren waren zu berücksichtigen. Die Markteinführung des nPA erweist sich als ein komplexer und langwieriger Prozess. Auch wenn sehr umfangreich, sorgt die gewählte Markteinführungsstrategie für die Ausnutzung der Stärken und für den Abbau der Schwächen, die mit dem nPA verbunden sind. Schließlich kann festgehalten werden, dass dank der Einführungsstrategie den Anwendungsmöglichkeiten für den nPA auf dem deutschen Markt kaum Grenzen gesetzt sind. Dies wird zur künftigen Entwicklung von Anwendungen seitens Unternehmen und Verwaltung führen. Die Ergebnisse der Marktanalyse stellen das Fundament für das wert- und mengenmäßige Marktwachstum, das seinerseits das zukünftige Marktpotenzial bestimmt.

4.4. eID-basierte Geschäftsmodelle

Es gibt zahlreiche Definitionen des Begriffs ‚Geschäftsmodell' in der Literatur. Laut Definition von Krcmar ist ein Geschäftsmodell eine „…Architektur für Produkt-, Service- und Informationsflüsse, einschließlich der Beschreibung der verschiedenen Akteure und ihrer Rollen sowie die Beschreibung potenzieller Gewinne/Leistungen für die verschiedenen Akteure und einer Beschreibung der Einnahmequellen" (Krcmar 2010, 435).

Bouwman (2002) definiert den Begriff Geschäftsmodell als „Beschreibung der Rollen und Beziehungen einer Firma, ihrer Kunden und Zulieferer als auch des Verkehrs von Gütern, Informationen und Geld zwischen diesen Parteien und den jeweiligen Hauptvorteilen für alle Beteiligten, insbesondere aber nicht ausschließlich für den Kunden". Fasst man alle diese Partner (Behörde, Bürger, Unternehmen, Intermediär) als Teilnehmer einer Wertschöpfungskette auf, beschreibt das Geschäftsmodell den Austausch zwischen diesen Teilnehmern sowie den jeweiligen Gewinn (monetär oder nicht monetär) dieser Partner (Peinel 2008, 31f).

Die in der Literatur existierenden Ansätze von Geschäftsmodellen beleuchten unterschiedliche Aspekte. Im Umfeld von E-Government sind neben ökonomischen Kennzahlen auch verschiedene Akteure relevant. Aus diesem Grund wird nachfolgend auf das Geschäftsmodell nach Peinel näher eingegangen.

4.4.1. E-Government-Geschäftsmodell nach Peinel

Für die Einführung von eID-Infrastrukturen wird in diesem Bericht die BMeG (Business Models for E-Government) Methode verwendet. BMeG unterstützt die Modellierung unterschiedlicher Wertschöpfungsketten mit einem besonderen Schwerpunkt auf E-Government-Dienste. BMeG geht von folgenden Prämissen aus (Peinel 2008, 64):

- Die Modellierung von Geschäftsmodellen stellt eine Wertschöpfungskette mit mehreren Partnern in gewissen Rollen dar. → Die BMeG Modellierung unterstützt insbesondere die Modellierung von Public Private Partnerships für E-Government-Dienste.
- PPP Partner sind bezüglich ihrer Kompetenzen komplementär in der Wertschöpfungskette organisiert. → Dies wird in der BMeG Methode durch das Konzept von Rollen realisiert.
- Die Modellierung erlaubt die Ablage von Finanzierungsoptionen wie Förderung, Sponsoring, Werbung, Transaktionsgebühren, Hosting, etc. → durch die Modellierung von Objektaustäuschen zwischen Partnern lassen sich unterschiedliche Finanzierungsoptionen in BMeG abbilden.
- Der finanzielle Aspekt und der Austausch von monetären Werten stehen nicht im Vordergrund, der Austausch von monetären Werten kann, muss aber nicht gegeneinander aufrechenbar sein. → Auch für kommerzielle Partner ist eine exakte Aufrechnung eines Geschäftsmodells zum Teil nicht möglich, denn eine Beteiligung an E-Government-Projekten kann auch als strategische Maßnahme im Sinne von Marketing oder Unterstützung anderer Dienste bewertet werden. In BMeG kann, muss aber kein Werteaustausch erfolgen.
- Insbesondere steht einem Aufwand für eine Dienstleistung nicht unbedingt ein monetärer Ausgleich gegenüber; da bspw. eine Behörde eine gesetzliche Verpflichtung besitzt, gewisse Aufwände auszuführen, kann die Leistung der Behörde auch kostenlos erfolgen. Somit bedeutet ein Austausch von Werten zwischen Partnern A und B nicht notwendigerweise, dass eine Gegenleistung von B nach A erfolgt. Zudem kann eine Gegenleistung auch von einem Partner C oder D erfolgen. → Bei der BMeG Modellierung kann, muss aber kein Rückobjekt für einen Werteaustausch modelliert werden.
- Jede Wertschöpfungskette liefert Vor- und Nachteile zur Einführung von Zielen der Partner. Eine Kette ist erfolgreich für einen individuellen Partner, wenn seine Vorteile überwiegen. Eine Kette ist erfolgreich für alle teilnehmenden Partner, wenn für alle Partner die Vorteile überwiegen (Win-Win-Situation). Auch können Mehrwerte nicht immer direkt zwei Entitäten im Modell zugeordnet werden (bspw. ist der Wert „Informiertheit des Bürgers" nicht direkt dem einzelnen Bürger zuzuordnen, desgleichen kann die Erfüllung einer Strategie oder einer Rechtsbestimmung keinen – für die Modellierung – relevanten Ursprung besitzen). Vor- und Nachteile könnten gewichtet werden. Desgleichen könnte es Ausschlusskriterien geben. → BMeG Modell und Editor unterstützen Argumente zur Teilnahme von Partnern, die als Vor-

und Nachteile modelliert werden. Vor- und Nachteile können Rollen oder Partnern zugeordnet sowie zwischen Partnern geteilt werden.

Das BMeG Modell beinhaltet folgende Modellierungsentitäten einer Wertschöpfungskette:

Name	Kurzbeschreibung
Wertschöpfungskette	Varianten eines E-Government-Dienstes mit verschiedenen Partnern
Partner	Beteiligte Organisation die in einer Wertschöpfungskette an einem Dienst teilnimmt
Rolle	Sammelbegriff für die Aufgabe der Organisation in einem Dienst
Objektaustausch	Austausch von Daten oder monetären Werten zwischen beteiligten Partnern in einer Wertschöpfungskette
Organisation	Ein Objekt einer realen Wert, das ein Unternehmen, eine Behörde oder einen Bürger in der Geschäftswelt darstellt
Politik	Entität, die die Ziele, Pläne und Vorgehensweisen eines Partners beschreibt
Vorteil	Ein Vorteil ist ein positives Argument eines Partners für die Teilnahme an einer Wertschöpfungskette
Nachteil	Ein Nachteil ist ein negatives Argument eines Partners für die Teilnahme an einer Wertschöpfungskette
Dienst/Service	Spezifikation der Dienste eines Partners oder einer Rolle

Tabelle 8: Modellierungsentitäten einer Wertschöpfungskette des BMeG Modells (Peinel 2008, 66ff)

Ein Dienst/Service im E-Government-Sektor wird durch unterschiedliche Partnerkombinationen und/oder unterschiedlichen Rollenkombinationen realisiert. Für alle beteiligten Partner bietet jede dieser Implementierungen Vor- und Nachteile. Des Weiteren wird jeder Partner durch eine Organisation dargestellt, welche eine bestimmte Rolle in der Wertschöpfungskette einnimmt und spezifische Dienste/Services leistet bzw. bietet und die zusätzlich durch ihre Teilnahme am Gesamtdienst diesen ergänzt bzw. verbessert (Peinel 2008, 67).

Zur Erfüllung des Dienstes können zwischen Partnern Objekte ausgetauscht werden, wie z. B. Daten oder monetäre Werte als Bezahlung für Einzeldienste in der jeweiligen Rolle. In der Wertschöpfungskette ist jeder Partner mindestens Objekterzeuger oder –empfänger, ansonsten wäre die Teilnahme des Partners an der Wertschöpfungskette ohne Mehrwert für den zu erbringenden Dienst. Des Weiteren hat jeder Partner Argumente (Vor- und Nachteile) für seine Teilnahme an der Wertschöpfungskette.

Diese Vor- und Nachteile beeinflussen eigene Geschäfts- bzw. Behördenpolitiken bzw. auch Politiken anderer Teilnehmer positiv oder negativ (Peinel 2008, 67).

4.4.2.Grafische Darstellung der BMeG Modellierungsmethode

Nachfolgend werden basierend auf der BMeG Modellierungsmethode nach Peinel die ausgewählten Anwendungsszenarien Kfz-Zulassung, ELSTER, Emissionshandel, Gewerbeanmeldung und Gesamtauskunft dargestellt.

4.4.2.1. *BMeG am Beispiel ‚Kfz-Zulassung'*

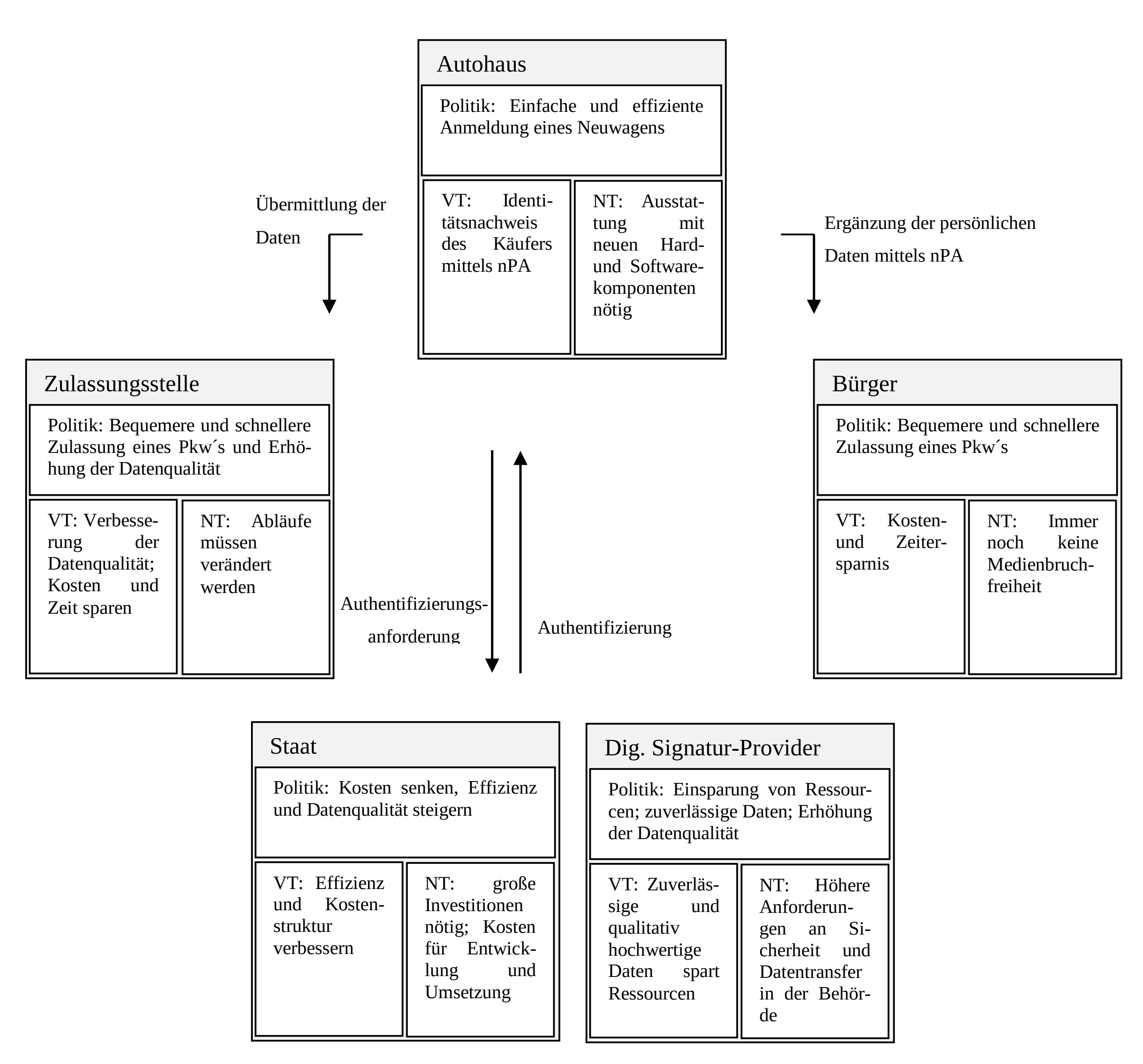


Abbildung 17: BMeG am Beispiel ‚Kfz-Zulassung' (Quelle: Eigene Darstellung)

4.4.2.2. *BMeG am Beispiel ‚ELSTER‘*

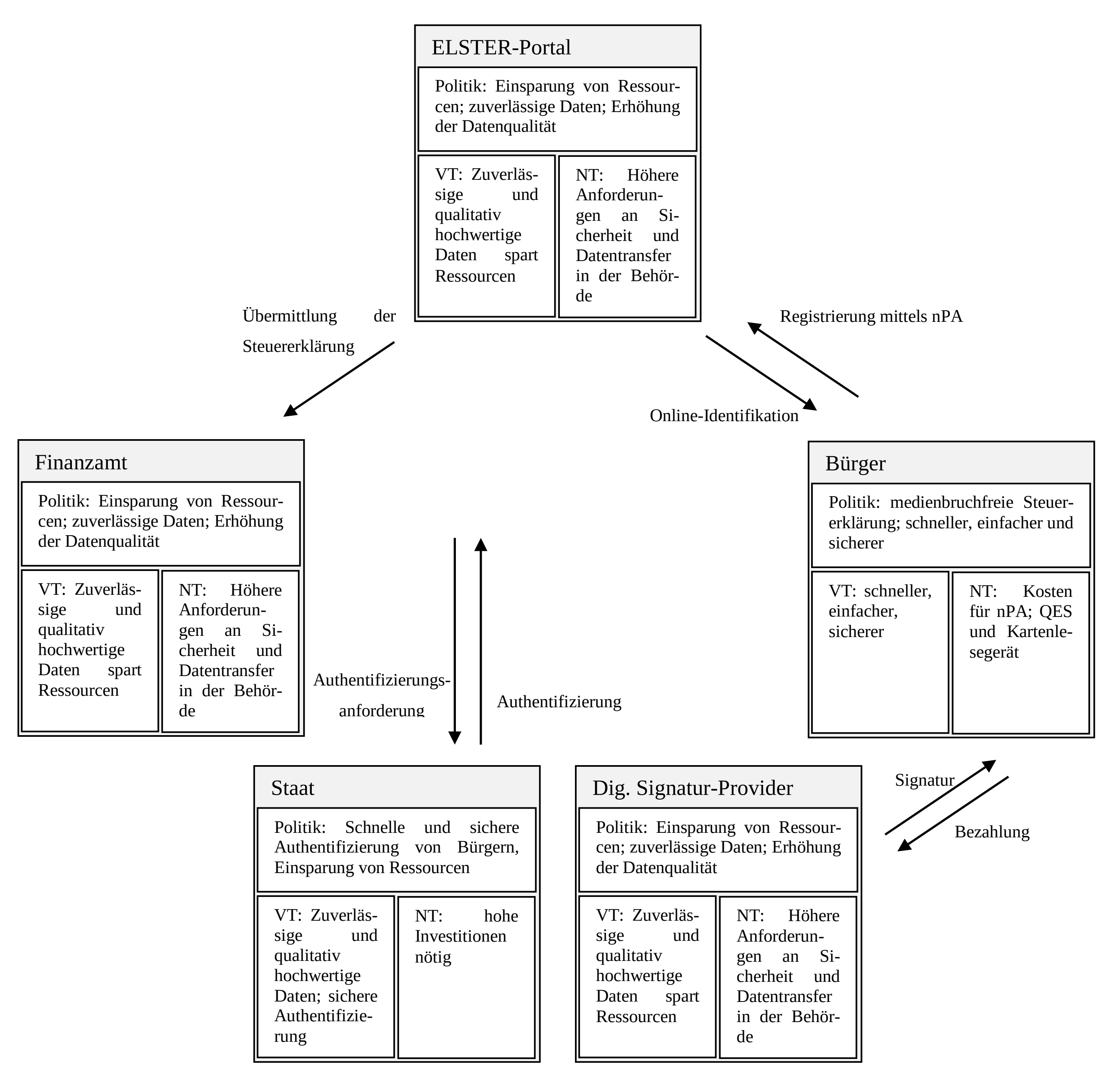


Abbildung 18: BMeG am Beispiel ‚ELSTER‘ (Quelle: Eigene Darstellung)

4.4.2.3. *BMeG am Beispiel ‚Emissionshandel‘*

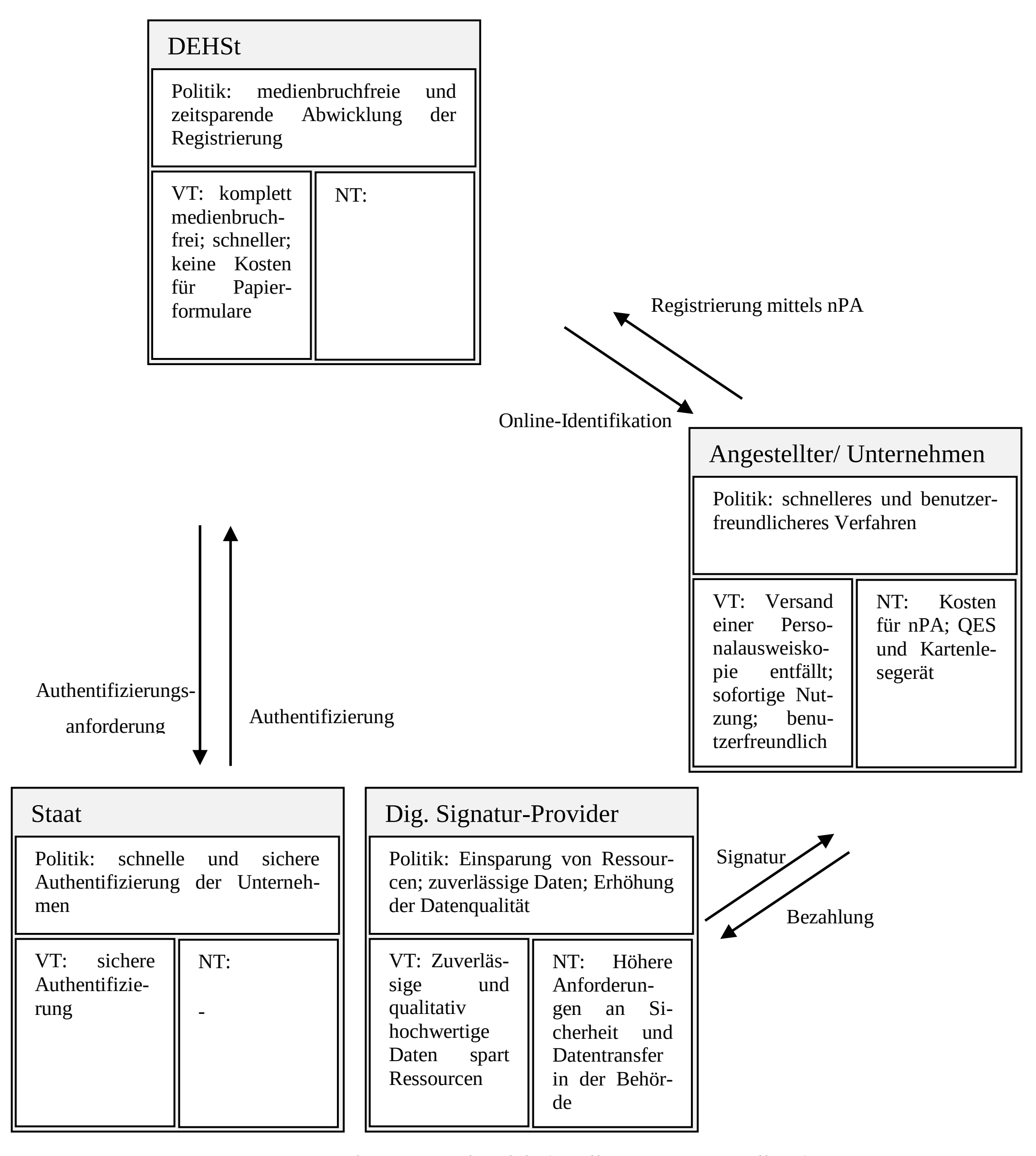


Abbildung 19: BMeG am Beispiel ‚Emissionshandel‘ (Quelle: Eigene Darstellung)

4.4.2.4. *BMeG am Beispiel ‚Gewerbeanmeldung‘*

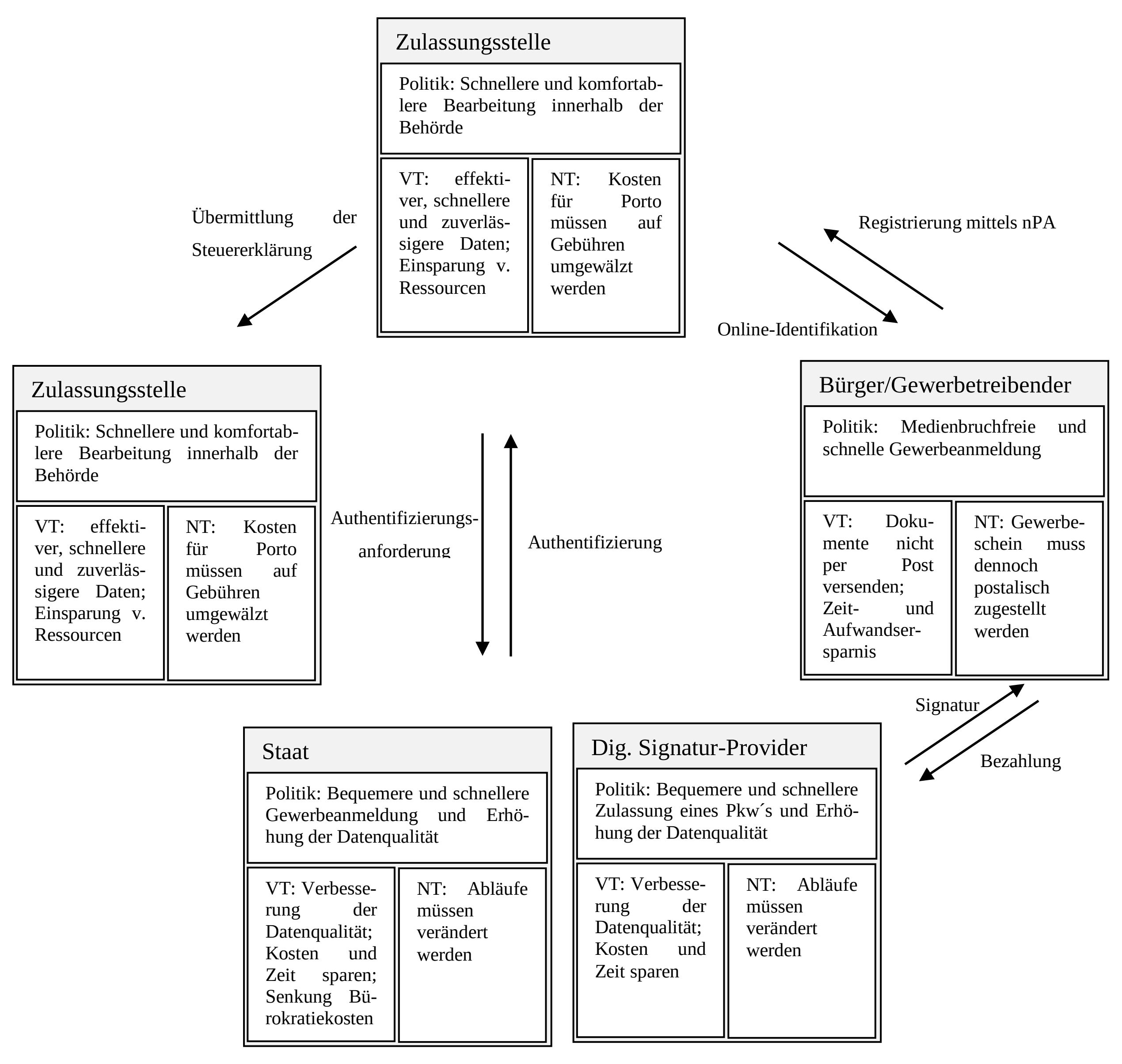


Abbildung 20: BMeG am Beispiel ‚Gewerbeanmeldung‘ (Quelle: Eigene Darstellung)

4.4.2.5. *BMeG am Beispiel ‚Gesamtauskunft‘*

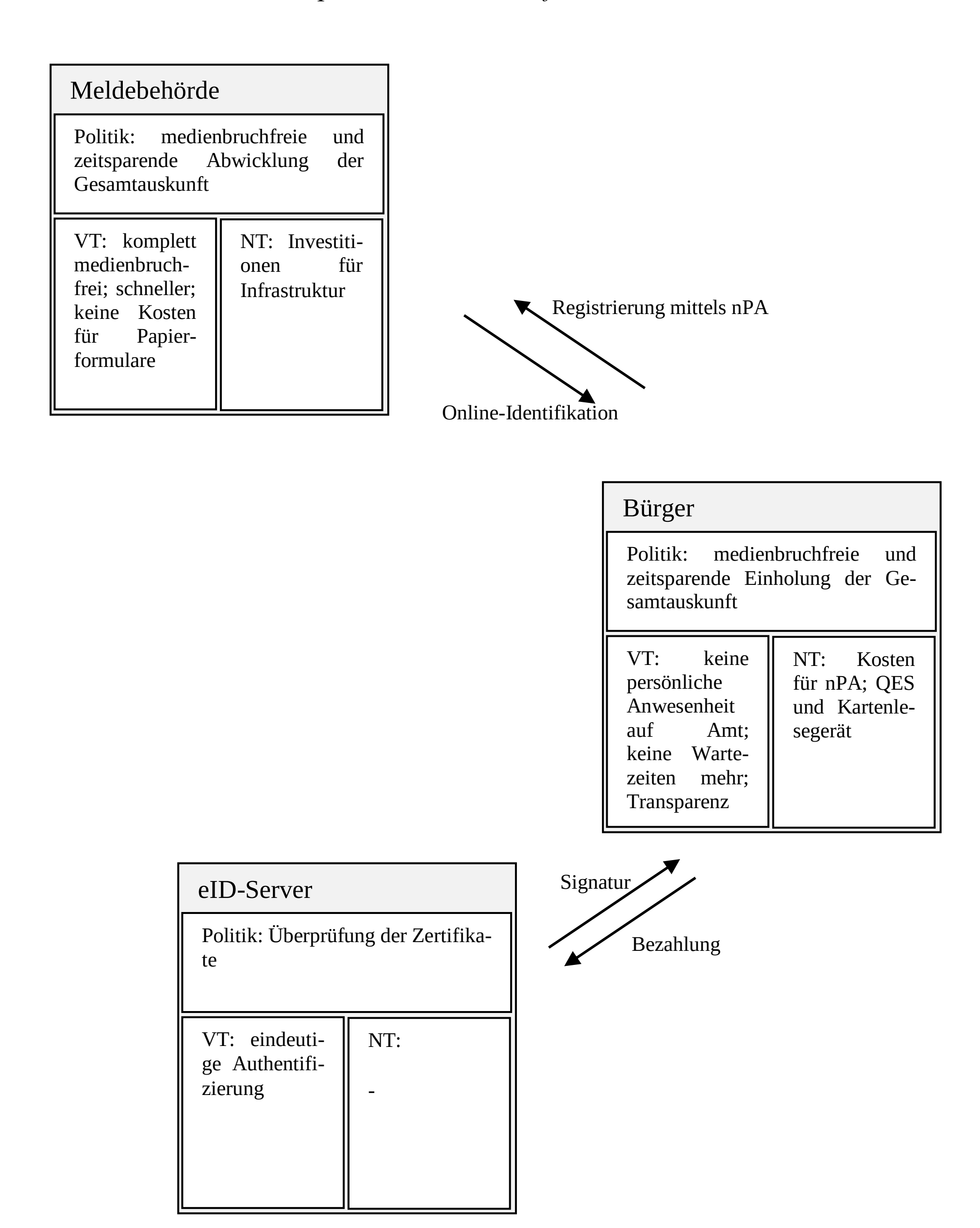


Abbildung 21: BMeG am Beispiel ‚Gesamtauskunft‘ (Quelle: Eigene Darstellung)

4.4.3. Kritische Erfolgsfaktoren für den Markteintritt

Die Kosten des neuen Personalausweises sind ein wichtiger Faktor für dessen Akzeptanz bei den Bürgern. Der Standardpreis des neuen Personalausweises mit digitalem Lichtbild beträgt 28,80 Euro, der nPA ist grundsätzlich für 10 Jahre gültig (Bundesministerium des Inneren 2010d). Zusätzlich kann der Ausweisbesitzer auf Wunsch, ohne weitere Kosten die eID-Funktion und zwei Fingerabdrücken hinzufügen lassen. Die wesentliche Komponente des neuen Personalausweises für fortgeschrittene E-Government-Dienste, die digitale Signatur, kann auf Wunsch des Ausweisinhabers gegen Aufpreis hinzufügt werden. Die zusätzlichen Kosten für die qualifizierte elektronische Signatur hängen vom jeweiligen Signaturanbieter ab (Bundesministerium des Inneren 2010d). Diese Funktionalität erlaubt es, Dienste, die ansonsten eine handgeschriebene Unterschrift des Ausweisbesitzers benötigten, online zu erledigen. Bei der Einführung des elektronischen Reisepasses gaben ebenfalls die Mehrkosten zum konventionellen Reisepass Anlass zu Diskussionen in Deutschland.



Abbildung 22: Komponenten des neuen Personalausweises (Bundesministerium für Wirtschaft und Technologie 2008, 8)

Durch Interviews mit Ansprechpartnern der Anwendungstestteilnehmer konnten weitere kritische Erfolgsfaktoren identifiziert werden:

- Die Dauer, bis alle (Melde)Behörden mit Soft- und Hardware ausgestattet sind.
- Technische Richtlinien sind noch nicht ausgereift und zertifiziert. Eine fehlende Zertifizierung schmälert die Akzeptanz.
- Lesegeräte: Nur Lesegeräte der Klasse 3 sind sicher, diese sind aber teuer.
- Fehlende Berechtigungszertifikate bzw. fehlende Auswahl des Zertifikatsanbieters.
- Das Verhältnis zwischen Anzahl der Ausweisinhaber und Anzahl der verfügbaren Dienste ist noch nicht ausgewogen.

4.5. eID-Anwendungsszenarien

Der Fokus in diesem Projekt liegt auf der Analyse der verschiedenen Szenarien, für die der nPA eingesetzt werden kann. Dies ist entscheidend für die Akzeptanz und beeinflusst auch den Markt und seine Teilnehmer.

Das Ziel der Regierung ist es, Vorteile für die Nutzung des neuen Personalausweises zu schaffen, die sonst nicht verfügbar sind. Die Marktsegmente sollten unterschieden werden – z. B. nach Student, Angestellter bzw. Bürger im Allgemeinen – und die möglichen Anwendungen des neuen Personalausweises sollten für diese Nutzer anhand von mehreren Szenarien definiert werden. Seit Oktober 2009 testen von der Regierung ausgewählte E-Business- und E-Government-Dienstleister die elektronische Identifikationsfunktion des neuen Ausweises in ihren Online-Diensten.

Die Regierung hat den Anwendungstest zweigeteilt, einerseits in zentrale Anwendungstests und andererseits in Anwendungstests, die für alle Firmen offen sind. In diesen Anwendungstests werden derzeit mehrere Szenarien getestet. Diese liefen bis Ende Oktober 2010 und ihre Ergebnisse sollten bei der Einführung des neuen Personalausweises im November 2010 verwendet werden.

Für den zentralen Anwendungstest wurden 30 Organisationen vom Bundesministerium des Inneren ausgewählt (Bundesministerium des Inneren 2009b) (vgl. Anhang Teil D).

Zusätzlich zum zentralen Anwendungstest, konnten auch Organisationen, die sich rechtzeitig registriert haben, Tests durchführen. Dieser Teil umfasste ungefähr 150 Organisationen (Bundesministerium des Inneren 2009a). Eine Aufstellung aller Organisationen wird im Anhang Teil E dargestellt. Im Rahmen des Projekts ist es nicht möglich, alle Szenarien zu analysieren. Deshalb wurde eine Anzahl von Szenarien ausgewählt, die im empirischen Teil des Projekts detailliert analysiert werden. Um die Szenarien für eine detaillierte Analyse auszuwählen, wurden diese nach ihrer Branche und Zielgruppe kategorisiert (vgl. Anhang Teil F).

Für eine detaillierte Analyse im Rahmen des Projekts wurde versucht repräsentative Fälle für die Beziehungen zwischen Behörden und Unternehmen (G2B) sowie zwischen Behörden und Bürgern (G2C) auszuwählen:

Name des Szenarios/ der Einrichtung	Test-Szenario	Anwendungstests	Bereich (e-Gov, e-Business,	X2X (G2B, G2C, B2B, C2C, usw.)	Sektor
Kfz					
Fraunhofer FOKUS	eKFZ	zentral	e-Gov	G2B, G2C	Antragswesen
ELSTER					
Bayerisches Landesamt für Steuern	Registirierungsverfahren für ELSTER	zentral	e-Gov	G2B, G2C	Steuer
Gewerbeanmeldung					
Datenzentrale Baden-Würtemberg (DZBW)	Online Gewerbeanzeige des Kommunalen Gewerbemanagements	zentral	e-Gov	G2B	Antragswesen
Emission					
DEHSt im Umweltbundesamt	Antrag auf Zuteilung von Emissionszertifikaten und Emissionsberichterstattung	zentral	e-Gov	G2B	Umwelt
Meldewesen					
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)	Gesamtauskunft über die gespeicherten Daten des Bürgers	zentral	e-Gov	G2C	Antragswesen

Abbildung 23: Ausgewählte Szenarien (Quelle: Eigene Darstellung)

4.5.1. Erhebung der Daten und Analyse der ausgewählten Szenarien (Methodik)

Die ausgewählten Szenarien werden in diesem Abschnitt im Detail beschrieben. Die dargestellten Beschreibungen und EPK[6]s wurden anhand einer quantitative Erhebung durchgeführt. Die Datenerhebung bestand aus folgenden Komponenten:

(1) Quantitative Befragung der Anwendungstestteilnehmer (Fragebogen und Experteninterviews)
(2) Prozesserfassung und –analyse der Szenarios EPKs vor und nach der nPA-Einführung
(3) Beobachtung hinsichtlich der Markteinführungsstrategie bei Bürgerbüros vor Ort

Hinsichtlich (3) konnte beobachtet werden, dass nur in Bürgerbüros für den neuen Personalausweises geworben wurde. Darüber hinaus wurden vereinzelte Werbespots im TV geschalten. Eine offensive Marketing- bzw. Werbungsstrategie konnte jedoch nicht beobachtet werden.

Zielgruppen der Untersuchung waren Teilnehmer der Anwendungstests. Dabei wurden folgenden Szenarios bzw. Anwendungstests ausgewählt (vgl. Abbildung 23):

(1) Kfz-Zulassung
(2) ELSTER
(3) Emissionshandel
(4) Gewerbeanmeldung

[6] EPK = „Ereignisgesteuerte Prozessketten (EPK) stellen die zeitlich-logischen Abhängigkeiten von Funktionen dar“ (Scheer 1997).

(5) Gesamtauskunft

Bei den jeweiligen Anwendungstestteilnehmern wurden Experteninterviews durchgeführt, auf Basis der Experteninterviews konnten die EPKs erstellt werden. Die Interviews wurden mittels zusammenfassender Inhaltsanalyse in diesen Projektbericht aufgenommen (Mayring 2010, 67ff).

4.5.1.1. *Kfz-Zulassung*

Das Szenario Online-Kfz-Zulassung wurde in einer Arbeitsgemeinschaft (ARGE eKfz) unter der Projektleitung des Fraunhofer-Instituts für Offene Kommunikationssysteme (kurz FOKUS) gemeinsam mit dem Zulassungsdienstleister Christoph Kroschke GmbH, der Daimler AG, Niederlassung Berlin, der ITDZ Berlin als Verwaltungs-IT-Infrastrukturdienstleister und der]init[AG durchgeführt (o. V. 2010a). Das Szenario Kfz-Zulassung mithilfe des nPA wurde im Testzeitraum ausschließlich in Berlin getestet.

Seit Ende 2010 sind die Tests abgeschlossen, und die Dienstleistung wird in den Autohäusern der Mercedes-Benz Niederlassung Berlin angeboten. Die Experten des Fraunhofer-Instituts für Offene Kommunikationssysteme arbeiten auch an der Festlegung eines Standards (xKfz) für einen XML-Datenaustausch (Fraunhofer Fokus 2010, 2). Insgesamt wurden im Jahr 2009 circa 20,6 Millionen Zulassungsvorgängen, d. h. Kfz-An-, Ab- und Ummeldungen (Deutschland-Online 2010) durchgeführt, 3,81 Millionen waren davon Kfz-Neuzulassungen (Kraftfahrt-Bundesamt 2009). Das Vorhaben ermöglicht eine einfache, flexible und Zeit und Aufwand sparende Gestaltung des Prozesses durch die Anwendung moderner Informationstechnologie (Deutschland-Online 2010).

Durch die Online-Zulassung soll nicht nur eine medienbruchfreie, komfortablere Abwicklungsmöglichkeit für Bürger geschaffen werden, sondern auch eine enorme Aufwandsreduzierung für Zulassungsstellen entstehen. Im Zusammenhang mit der Verknüpfung der derzeit technischen Möglichkeiten und den fachpolitischen, rechtlichen und organisatorischen Grundvoraussetzungen bildet die Generierung eines beidseitigen Nutzen den wichtigsten Erfolgsfaktor für das Vorhaben ‚Kfz-Wesen' (Deutschland-Online 2009, 1). Dabei wird der Staat davon profitieren, dass die „[...] Effizienz und Kostenstruktur der Zulassungsverwaltung verbessert werden" (Deutschland-Online 2010). Der Weg zu Einführung von E-Government Dienstleistungen verlangt gravierende organisatorische Änderungen (Bundesamt für Sicherheit in der Informationstechnik 2005, 4). Weiter ist mit der Modernisierung der Kfz-Anmeldung auch die Berücksichtigung der Interessen und Anforderungen aller Beteiligten verbunden (Kommune21 2010). Im Folgenden wird untersucht, wie die Kfz-Zulassung ohne Verwendung des neuen Personalausweises bis heute abläuft. Parallel zum konventionellen Verfahren soll die Online-Zulassung, die durchgängig online ausgeführt wird, angeboten werden. In einem Vergleich des bisherigen Verfahrens mit dem Vorgang unter Verwendung des nPA werden anschließend die dadurch eröffneten Möglichkeiten geschildert.

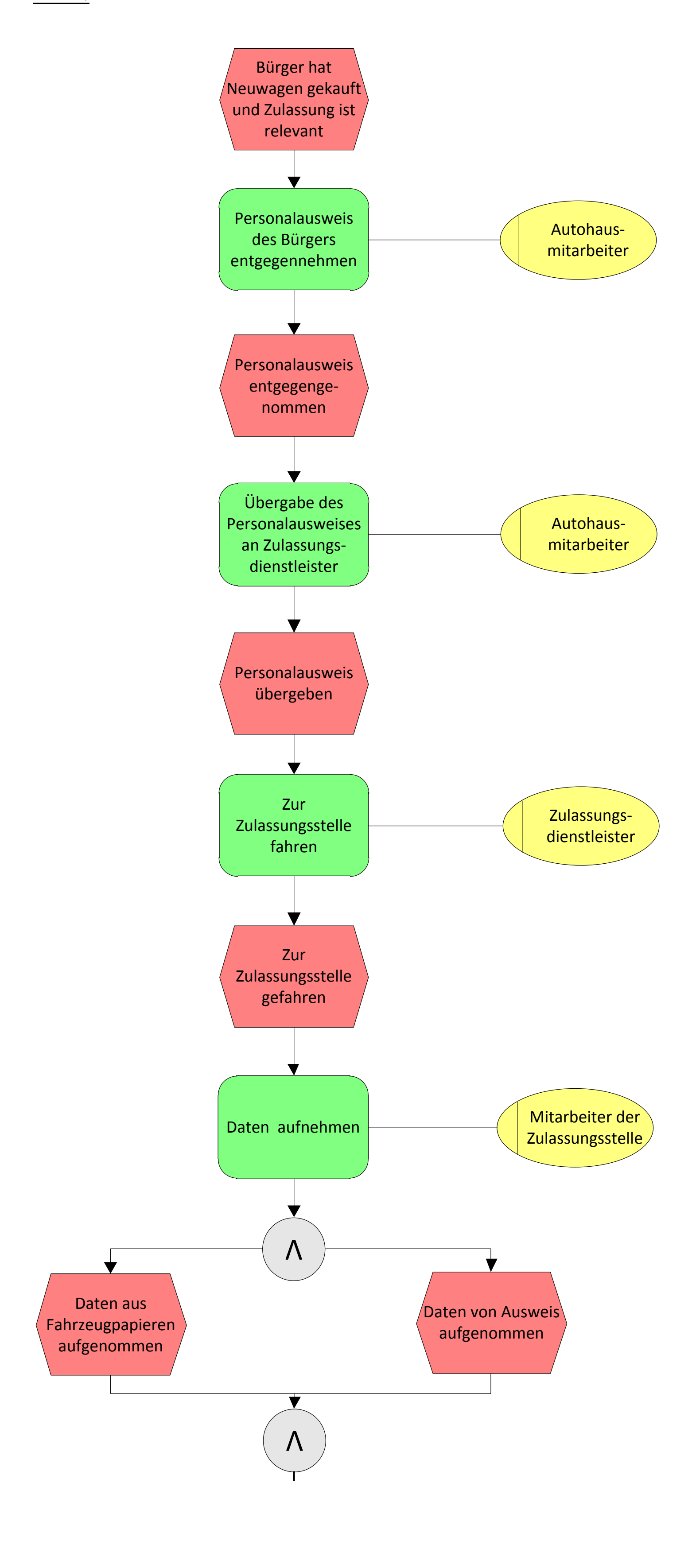
Kfz-Zulassung ohne nPA

Die Tönjes Holding AG bietet Bürgern bereits die teilweise Abwicklung der Kfz-Zulassung über das Internet an. Derzeit werden die nötigen Unterlagen beim Bürger durch Logistikunternehmen (z. B. UPS-Kurier) abgeholt und die Fahrzeugpapiere sowie die Kennzeichen mit Siegel nach der Ausstellung beim zuständigen Amt an die Bürger zurückgesendet (Tönjes Holding AG 2010b).

Bürger haben im ersten Schritt die Möglichkeit, die gewünschte Dienstleistung (Fahrzeug-, Oldtimer- oder Saison-Zulassung) auszuwählen. Im zweiten Schritt wird das Format des Kennzeichens durch die Wahl des Fahrzeugtyps bestimmt (Pkw, Motorrad, Lkw oder Quad). Die Region wird durch Eingabe der Postleitzahl in Schritt drei festgelegt. Nun besteht die Möglichkeit die restlichen Buchstaben und Ziffern zufällig generieren zu lassen, ein Wunschkennzeichen anzugeben oder ein bereits reserviertes Kennzeichen über einen Reservierungs-Code freizuschalten. Anschließend werden den Bürgern alle notwendigen Dokumente (Fahrzeugpapiere, Versicherungsnachweis, Personalausweis, Vollmacht für Tönjes), die für den UPS-Kurier bereitgehalten werden müssen, aufgezeigt. Nach der Online-Bezahlung und der Angabe der persönlichen Daten ist der Bestellvorgang abgeschlossen (Tönjes Holding AG 2010c). Im letzten Schritt werden die vom Logistikpartner abgeholten Unterlagen bearbeitet und nach erfolgreicher Zulassung die Schilder und Kfz-Papiere dem Nutzer zugestellt. Die Tönjes Holding AG gibt 72 Stunden als den für den gesamten Prozess notwendigen Zeitaufwand an (Tönjes Holding AG 2010c).

Weiterhin besteht ebenso die Möglichkeit, eine Kfz-Zulassung persönlich bei der Zulassungsbehörde vorzunehmen. Dabei wird der komplette Vorgang vom Verwaltungsmitarbeiter bearbeitet. Anschließend bekommt der Bürger seine Kfz-Papiere ausgehändigt und kann sich die Nummernschilder prägen lassen.

EPK:



Bürger hat Neuwagen gekauft und Zulassung ist relevant
Personalausweis des Bürgers entgegennehmen
Autohaus-mitarbeiter
Personalausweis entgegenge-nommen
Übergabe des Personalausweises an Zulassungs-dienstleister
Autohaus-mitarbeiter
Personalausweis übergeben
Zur Zulassungsstelle fahren
Zulassungs-dienstleister
Zur Zulassungsstelle gefahren
Daten aufnehmen
Mitarbeiter der Zulassungsstelle
Λ
Daten aus Fahrzeugpapieren aufgenommen
Daten von Ausweis aufgenommen
Λ

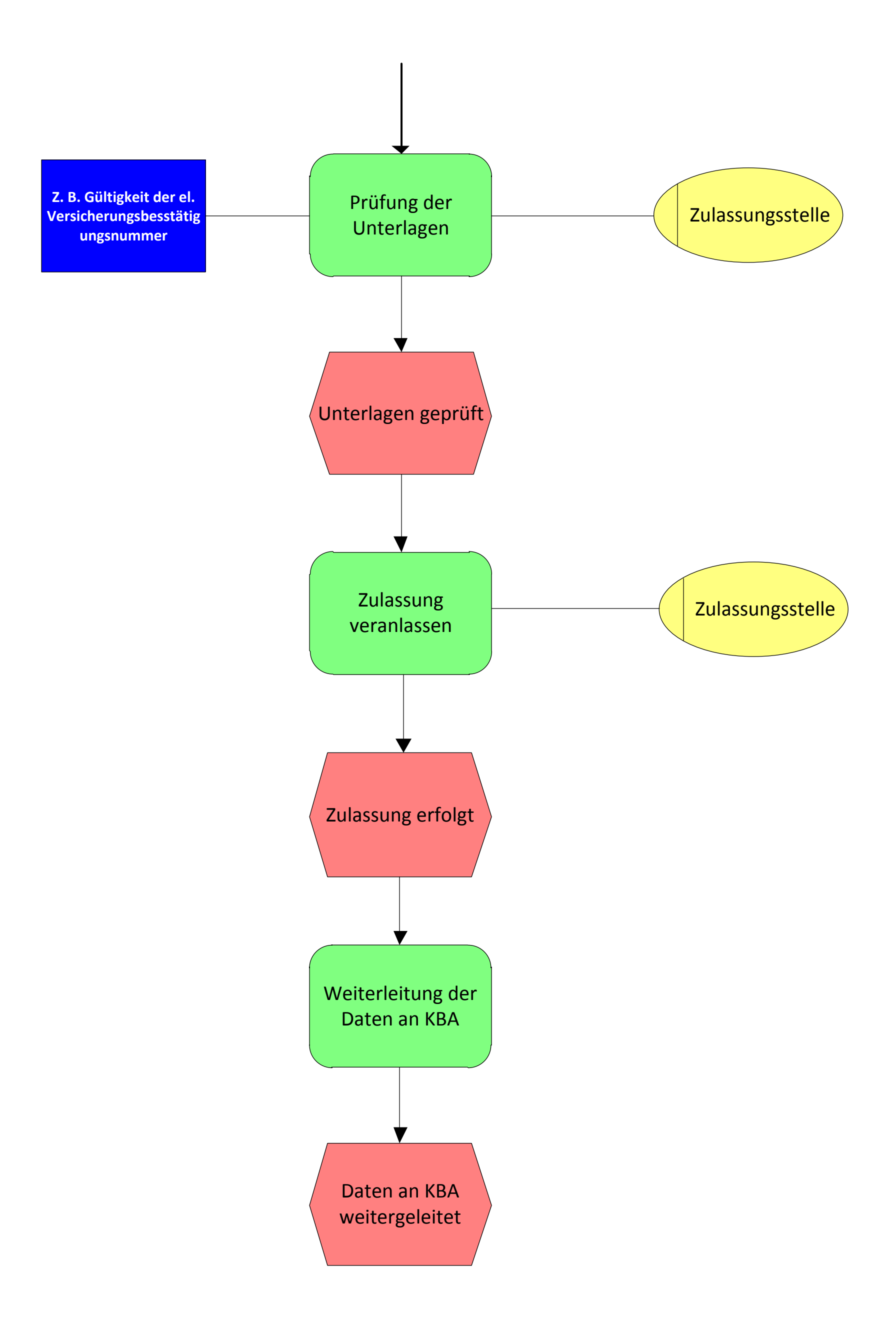


Abbildung 24: EPK der Kfz-Zulassung ohne nPA (Quelle: Eigene Darstellung)

Kfz-Zulassung mit nPA

Die Kfz-Zulassung mithilfe des nPA kann auf zwei Weisen erfolgen. Zum einen kann die neue Web 2.0 Internet-Plattform ‚Tönjes-Portal' genutzt werden, die für die Anwendung des nPA entwickelt wurde. Zum anderen ist die Übermittlung der Identitäts- und Fahrzeugdaten über ein Portal im Autohaus möglich (Tönjes Holding AG 2010a, 1).

Durch den Einsatz des nPA im ‚Tönjes-Portal' kann in der ersten Stufe der Umsetzung keine Medienbruchfreiheit sichergestellt werden. Da die Fahrzeugdokumente in Papierform sind, ist es aus rechtlichen und polizeilichen Gründen erforderlich, dass diese durch Logistikpartner vom und zum Bürger transportiert werden (Deutschland-Online 2009, 2). Allerdings können durch den Einsatz des nPA die

persönlichen Daten zuverlässiger als in Form eines Formulars aufgenommen werden, was den Prozess beschleunigt. Die zweite Stufe soll in Zukunft eine Medienbruchfreiheit ermöglichen, indem die Fahrzeugdokumente durch elektronische ersetzt werden (Deutschland-Online 2010).

In der ersten Stufe wurde die tatsächliche Umsetzung der Datenübermittlung vom Autohaus realisiert. Der Käufer legt seinen nPA auf das Kartenlesegerät im Autohaus. Nachdem er auf einem Bildschirm gesehen hat, welche Daten ausgelesen werden müssen, bestätigt er dies und gibt seine sechsstellige PIN ein. Die persönlichen Daten werden über das IT-Dienstleistungszentrum (ITDZ) Berlin, ein eID-Server, überprüft. Parallel dazu läuft die Speicherung der Antragsdaten über das ZDL Portal. Zu diesem Portal werden auch die überprüften persönlichen Daten gesendet. Anschließend werden alle Informationen, Antragsdaten und persönliche Daten, gemeinsam zur Zulassungsbehörde (das Landesamt für Bürger- und Ordnungsangelegenheiten, auch LABO) transferiert. Über die optimierte Zustellungslogistik des Dienstleisters werden die Fahrzeugpapiere und Kennzeichen in physischer Form zum Autohaus gebracht (siehe Abbildung 25).

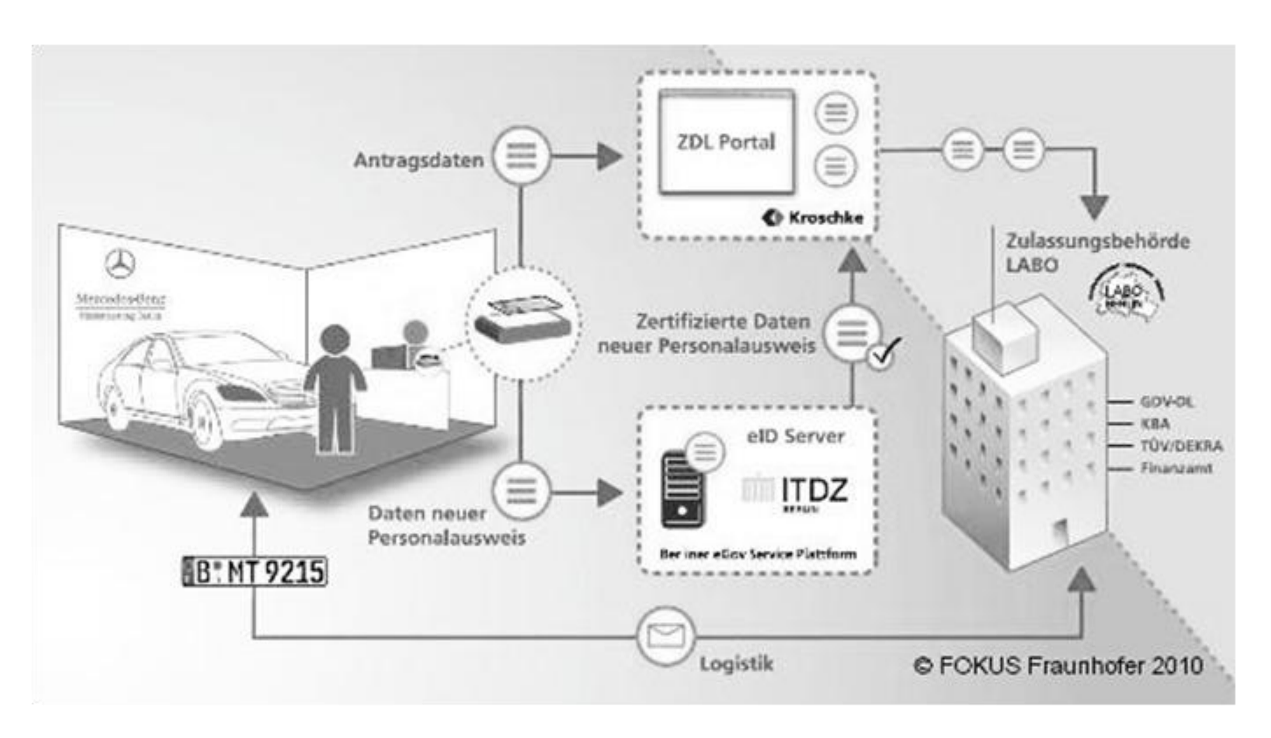
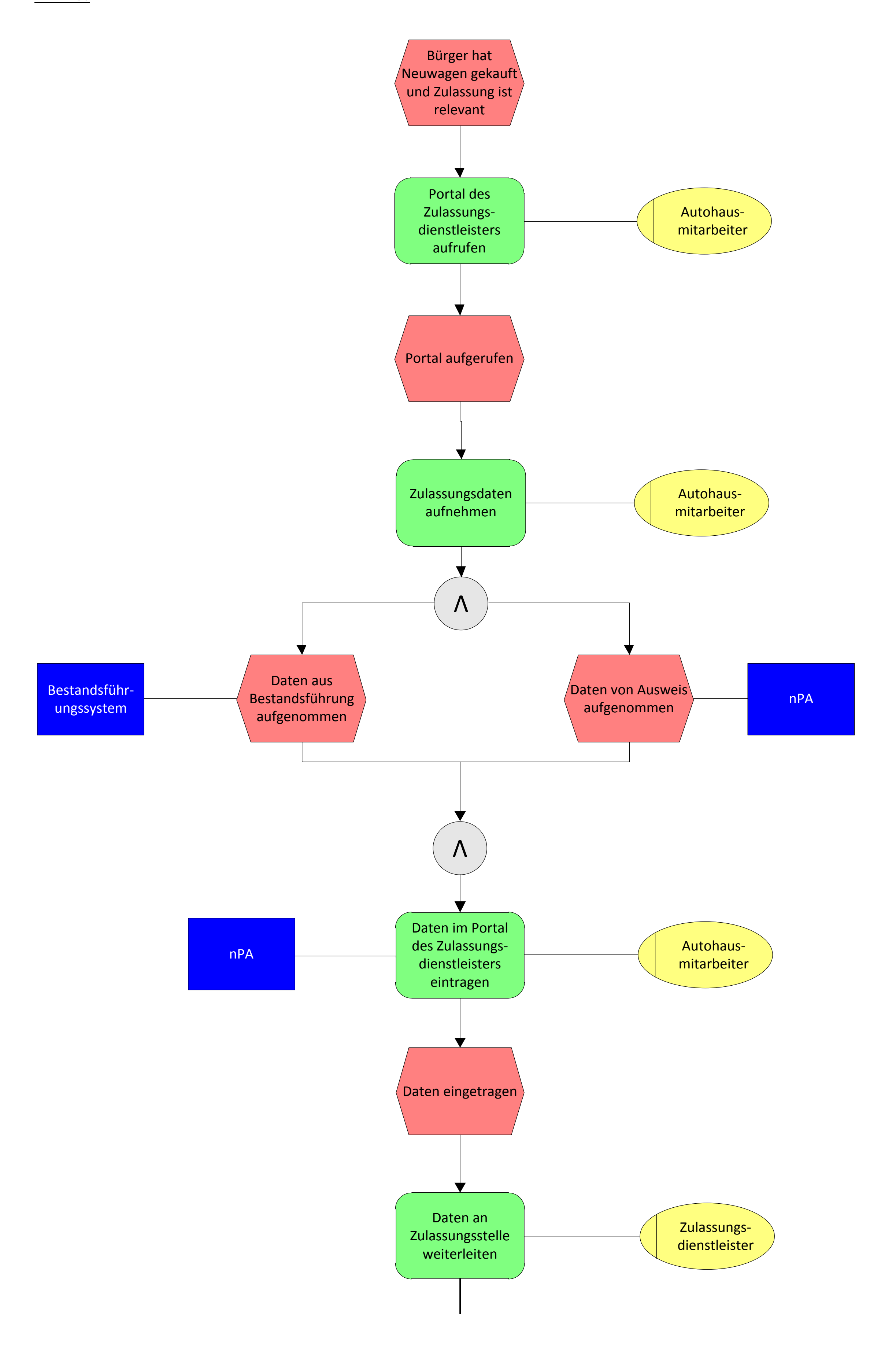


Abbildung 25: Kfz-Zulassung mittels nPA (Quelle: In Anlehnung an (Löhe/Tschichholz 2010)

EPKs:


Bürger hat Neuwagen gekauft und Zulassung ist relevant
Portal des Zulassungs-dienstleisters aufrufen
Autohaus-mitarbeiter
Portal aufgerufen
Zulassungsdaten aufnehmen
Autohaus-mitarbeiter
Λ
Bestandsführ-ungssystem
Daten aus Bestandsführung aufgenommen
Daten von Ausweis aufgenommen
nPA
Λ
nPA
Daten im Portal des Zulassungs-dienstleisters eintragen
Autohaus-mitarbeiter
Daten eingetragen
Daten an Zulassungsstelle weiterleiten
Zulassungs-dienstleister

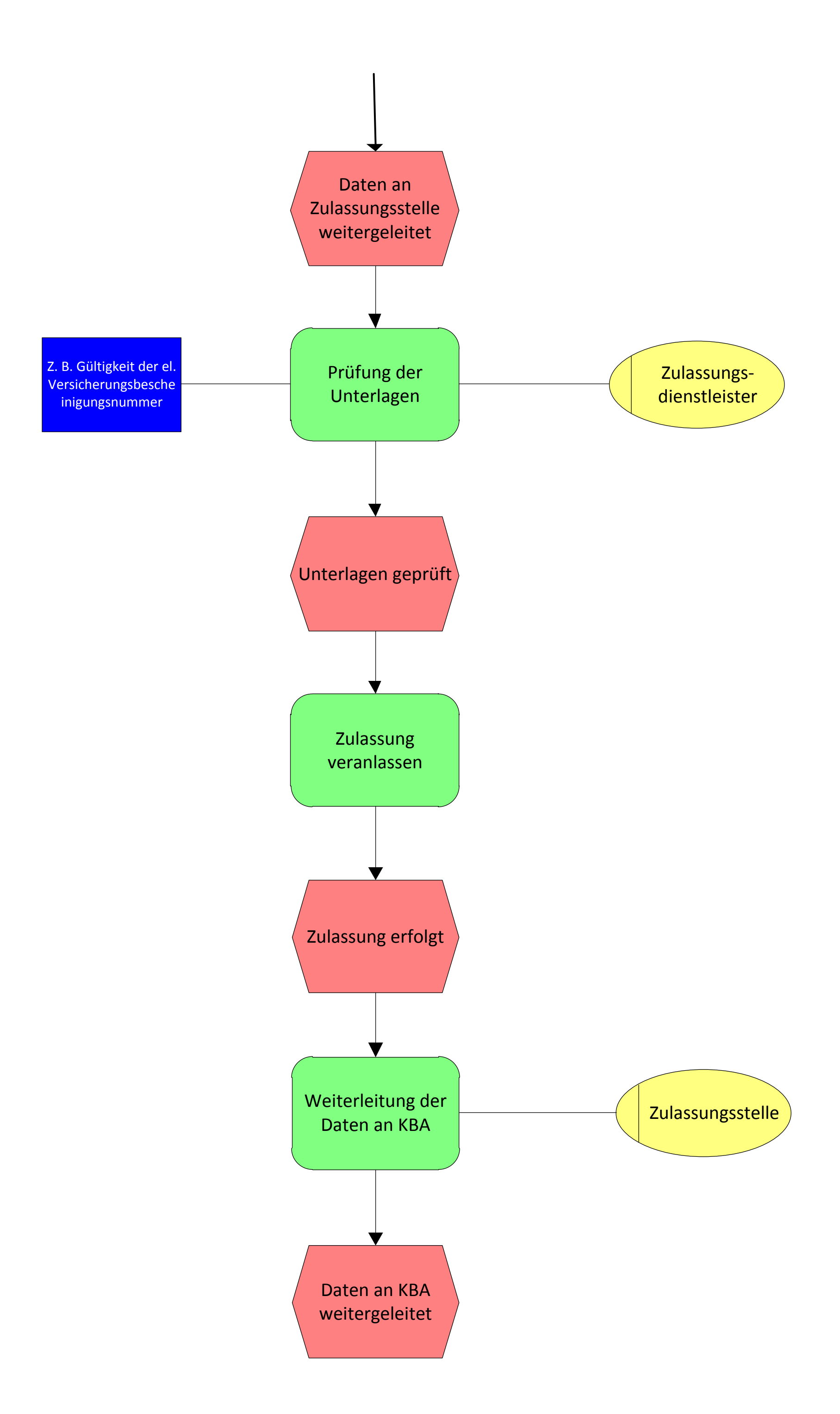


Abbildung 26: EPK der Kfz-Zulassung nach nPA-Einführung (Quelle: Eigene Darstellung)

Ausblick

Auf Grundlage der Ergebnisse und Fortschritte aus Stufe 1 sollen ab 2013 in Stufe 2 die Weiterentwicklung der IT-Verfahren, sowie beispielsweise der Einsatz elektronischer bzw. elektronisch lesbarer Fahrzeugdokumente erprobt werden, um Medienbrüche vollständig vermeiden zu können. Diesbezüglich sind jedoch noch weitere rechtliche Änderungen vorzunehmen und organisatorische Ansätze zur elektronischen Abwicklung zu untersuchen (Deutschland-Online 2009, 7f). Ab 2012 sollen die Fahrzeugdokumente durch elektronisch aus- und einlesbare Medien ersetzt werden. Das stellt die zweite Stufe des Projekts dar und sorgt für Medienbruchfreiheit. Dabei sollen alle Aspekte geprüft werden, insbesondere der Verkehrssicherheit, Missbrauchsverhinderung und der Wirtschaftlichkeit (Deutschland-Online 2010).

4.5.1.2. *ELSTER*

In der Bevölkerung nimmt die Akzeptanz, die Einkommensteuererklärung online abzuwickeln immer mehr zu. So übermittelten im Jahr 2009 bereits 8,3 Millionen Bürger ihre Steuererklärung mittels ELSTER (Bayerisches Landesamt für Steuern 2010b). Durch die Einführung des neuen Personalausweises soll auch bei der elektronischen Steuererklärung komplett auf physische Dokumente verzichtet werden. Hierbei gibt es drei verschiedene Pakete, aus denen bei der Registrierung gewählt werden kann – ELSTER*Basis*, ELSTER*Spezial* und ELSTER*Plus*. Diese unterscheiden sich lediglich im Signaturverfahren (Bayerisches Landesamt für Steuern 2010a). Bei der Verwendung von ElsterPlus, das Verfahren mit der höchsten Sicherheitsstufe, wird eine Signaturkarte benutzt (Finanzamt 2010, 1). Mit Verfügbarkeit des nPA werden die Elster-Online-Zertifikate abgelöst (Bundesministerium des Inneren 2008, 49). Etwa 56 % der deutschen Bürger möchte den neuen Personalausweis bei der elektronischen Steuererklärung (ELSTER) nutzen (siehe Abbildung 8). Im Folgenden wird die Datensicherheit bei der Nutzung des ElsterOnline-Portals mit und ohne nPA verglichen.

Registrierung bei ELSTEROnline ohne nPA

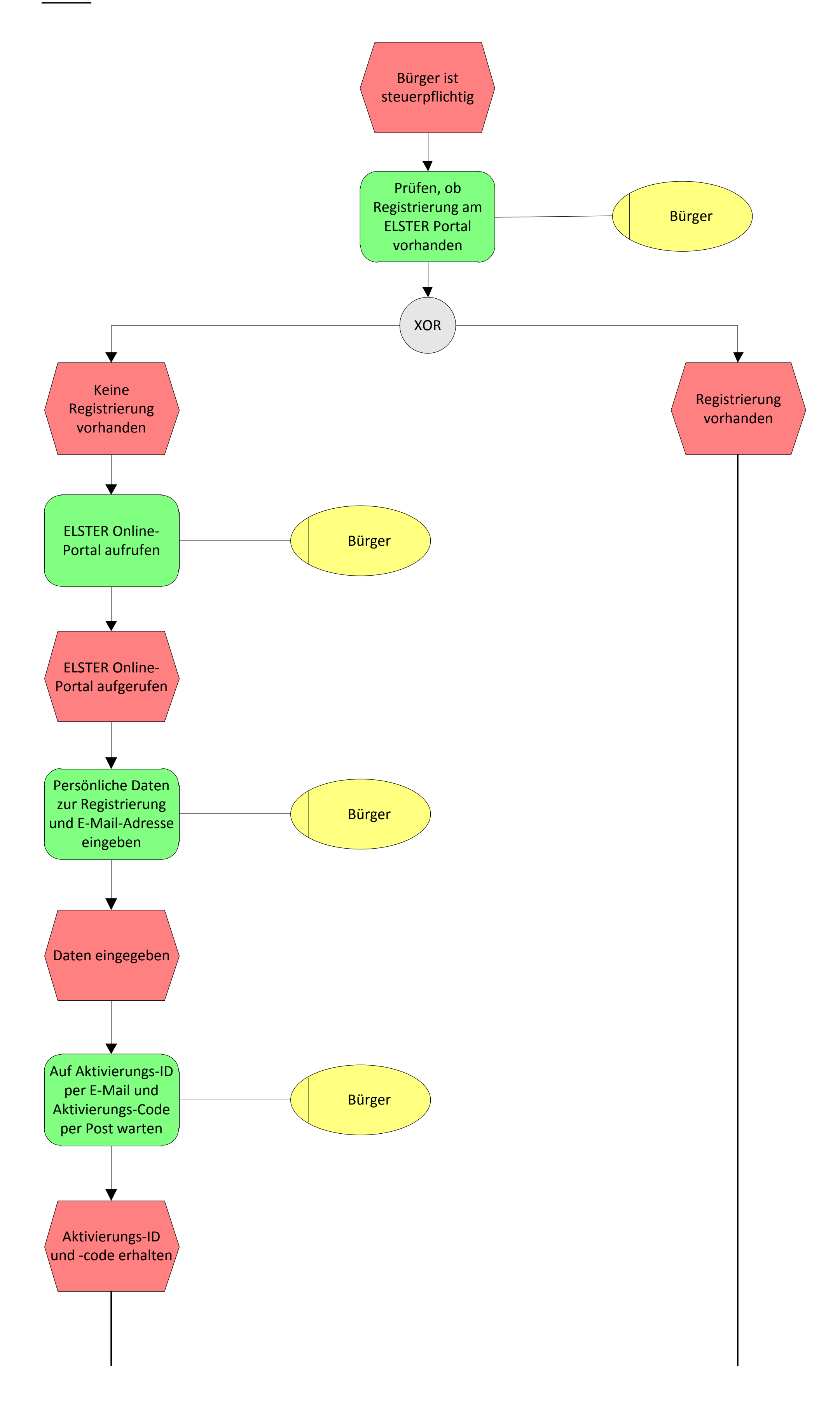
Den Nutzern stehen drei Registrierungsmöglichkeiten zur Verfügung. Zum einen gibt es die Basis- und die Spezial-Anmeldung. Hierbei wird das Zertifikat dem Bürger zugesandt. Beim ELSTERBasis wird dieses auf dem Rechner des Nutzers und bei ELSTERSpezial auf einem sog. ELSTER-Stick (ein Kryptochip) gespeichert. Bei ELSTERPlus wird das Zertifikat auf der Signaturkarte des Nutzers gespeichert, um die Mobilität und die Sicherheit zu erhöhen (Bayerisches Landesamt für Steuern 2010a).

Die Registrierung bei ELSTEROnline kann in drei Schritte aufgeteilt werden, wobei der letzte Schritt das erstmalige Einloggen ist. Im ersten Schritt gibt der Nutzer seine persönlichen Daten (u. a. die Steuernummer und eine E-Mail-Adresse) und ggf. Daten seines Unternehmens an. Dann kann er zwi-

schen zwei Zertifikaten auswählen – persönlichen und nicht-persönlichen (Finanzamt 2010, 2). Diese Wahl wirkt sich nur auf die Art aus, wie der Nutzer von der Behörde gesehen wird – als natürliche Person oder als Organisation/Unternehmen. Bei der Wahl des persönlichen Zertifikats wird ein Aktivierungsbrief von der zuständigen Finanzverwaltung an die Postadresse, die für diese Person und Steuernummer im Grundinformationsdienst gespeichert ist, gesendet. Bei der Wahl eines Organisationszertifikats sind neben der Umsatzsteuer-Voranmeldung und sonstigen Bescheinigungen auch die Berechtigungsdaten anzugeben (Finanzamt 2010, 1ff). Der Aktivierungsbrief wird dann an die Adresse der Organisation verschickt. Der erste Schritt wird unabhängig von der Wahl zwischen ELSTER*Basis*, ELSTER*Spezial* und ELSTER*Plus* durchgeführt.

Der zweite Schritt ist das Aktivieren des Zugangs mit dem postalisch erhaltenen Aktivierungs-Code. Wenn man ELSTER*Plus* verwendet, wird das Zertifikat aus der Signaturkarte bei ELSTER gespeichert und so kann sich der Nutzer einloggen. Bei Verwendung der Basis- oder Spezial-Version wird vom Nutzer eine PIN-Nummer ausgestellt und von ELSTER ein vorläufiges Zertifikat. Diese werden dann ausgetauscht. Beim erstmaligen Einloggen wird das vorläufige Zertifikat durch ein endgültiges überschrieben und erst dann kann eine authentifizierte Übermittlung erfolgen (Finanzamt 2010, 1ff).

EPK:


Bürger ist steuerpflichtig
Prüfen, ob Registrierung am ELSTER Portal vorhanden
Bürger
XOR
Keine Registrierung vorhanden
Registrierung vorhanden
ELSTER Online-Portal aufrufen
Bürger
ELSTER Online-Portal aufgerufen
Persönliche Daten zur Registrierung und E-Mail-Adresse eingeben
Bürger
Daten eingegeben
Auf Aktivierungs-ID per E-Mail und Aktivierungs-Code per Post warten
Bürger
Aktivierungs-ID und -code erhalten

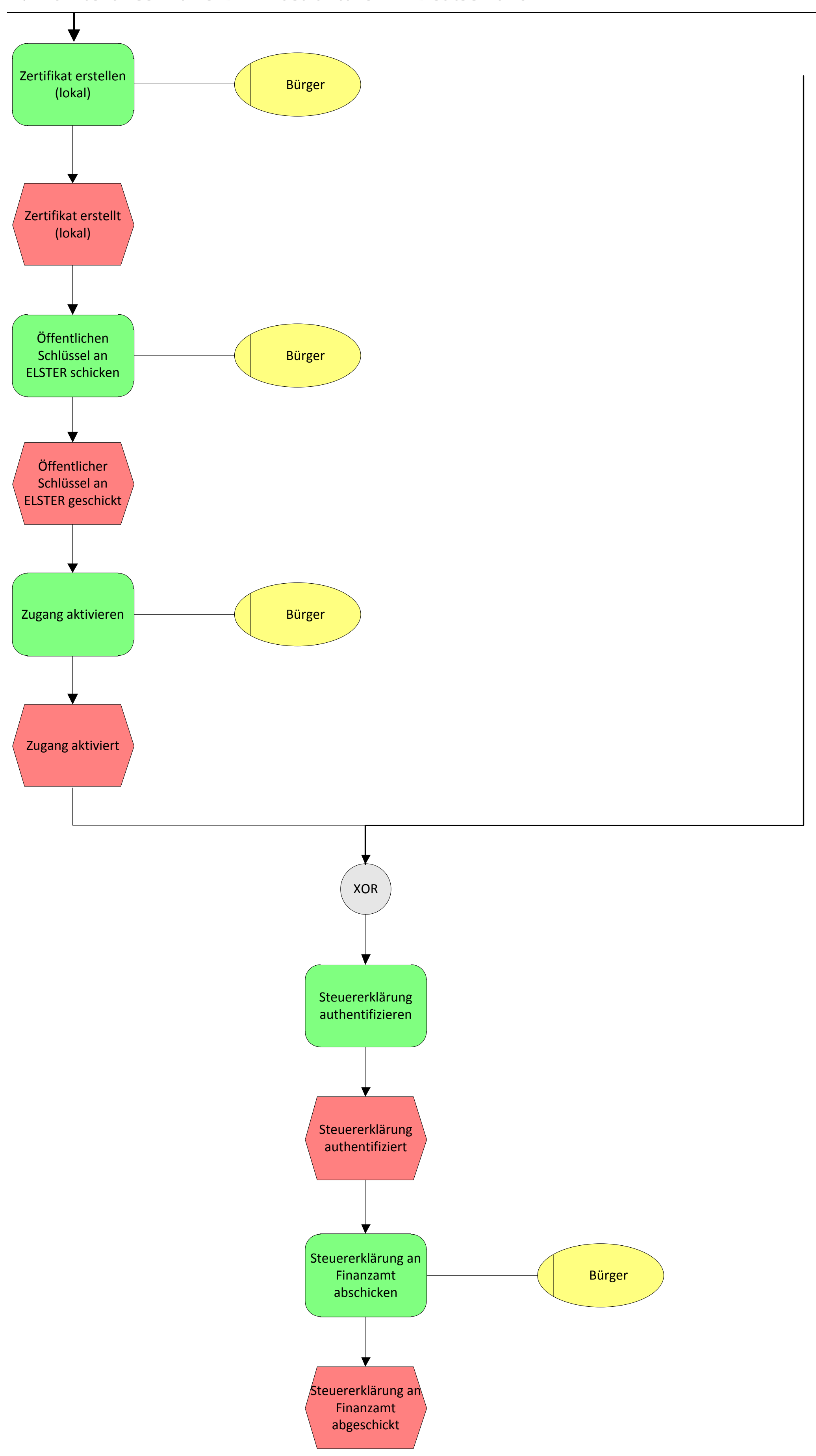
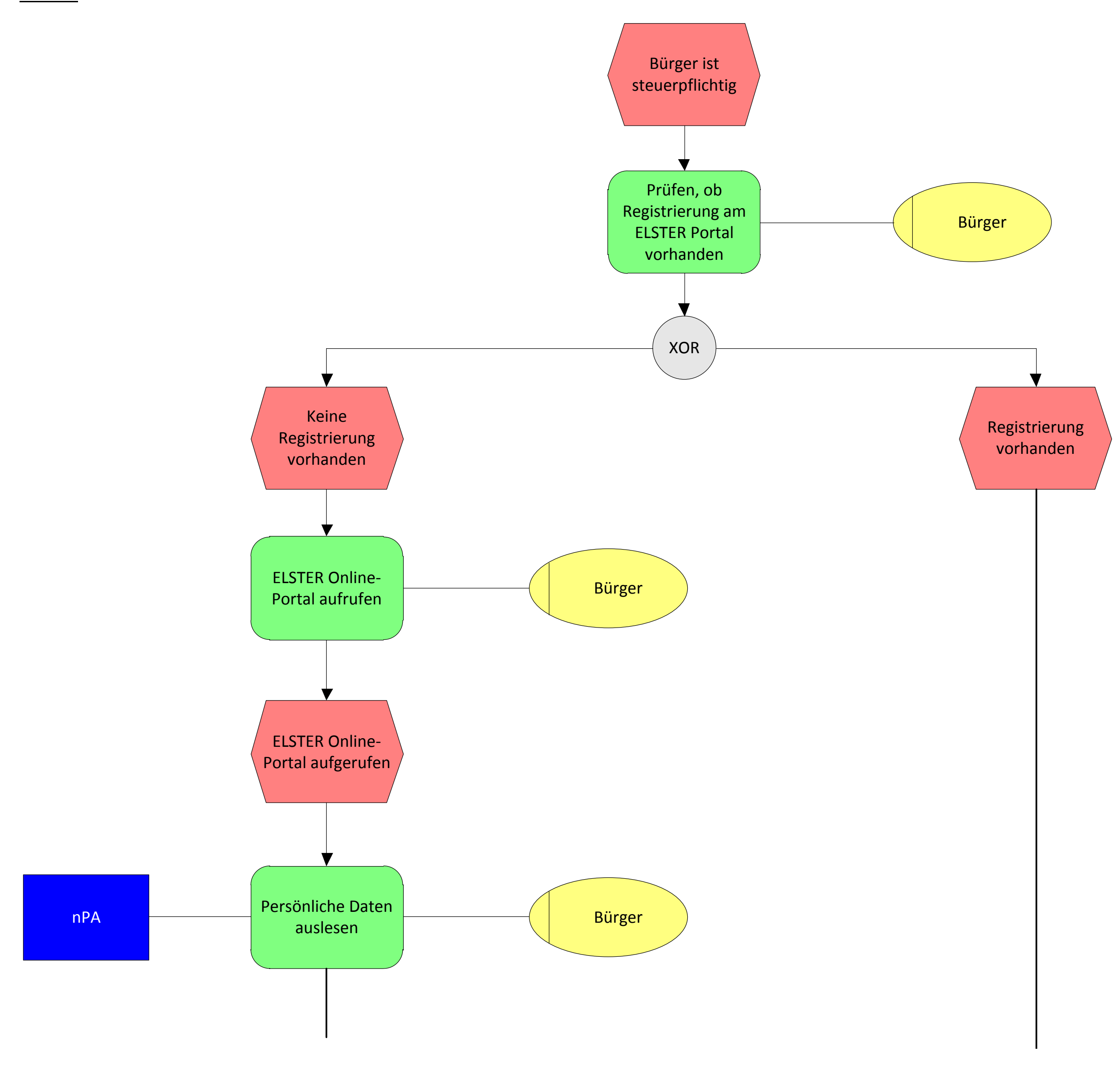


Abbildung 27: EPK vor nPA-Einführung (Quelle: Eigene Darstellung)

Registrierung beim ELSTEROnline mit nPA

Durch die Integration des nPA bei den ELSTEROnline-Verfahren wird der postalische Versand des Aktivierungscodes durch einen Identitätsnachweis mittels neuen Personalausweises ersetzt (Behörden Spiegel Online 2010). Dies ist eine wesentliche Verbesserung im Vergleich zum bisherigen Verfahren, da dadurch eine höhere Sicherheit und Benutzerfreundlichkeit angeboten wird. Bisher gab es eine Auswahl zwischen drei Sicherheitsstufen, repräsentiert durch die drei Profile (ELSTER*Basis*, ELSTER*Spezial* und ELSTER*Plus*) (Finanzamt 2010, 1ff). Durch den Einsatz der eID-Funktion des nPA werden die gesondert zu beantragende Zertifikate durch den auf dem nPA vorhandenen Zertifikat ersetzt (Bundesministerium des Inneren 2008, 49). Dies korrespondiert zu der höchsten Sicherheitsstufe bisher – ELSTER*Plus*. Der nPA wird folglich auch als Signaturkarte verwendet (Bundesministerium des Inneren 2008, 49).

EPK:



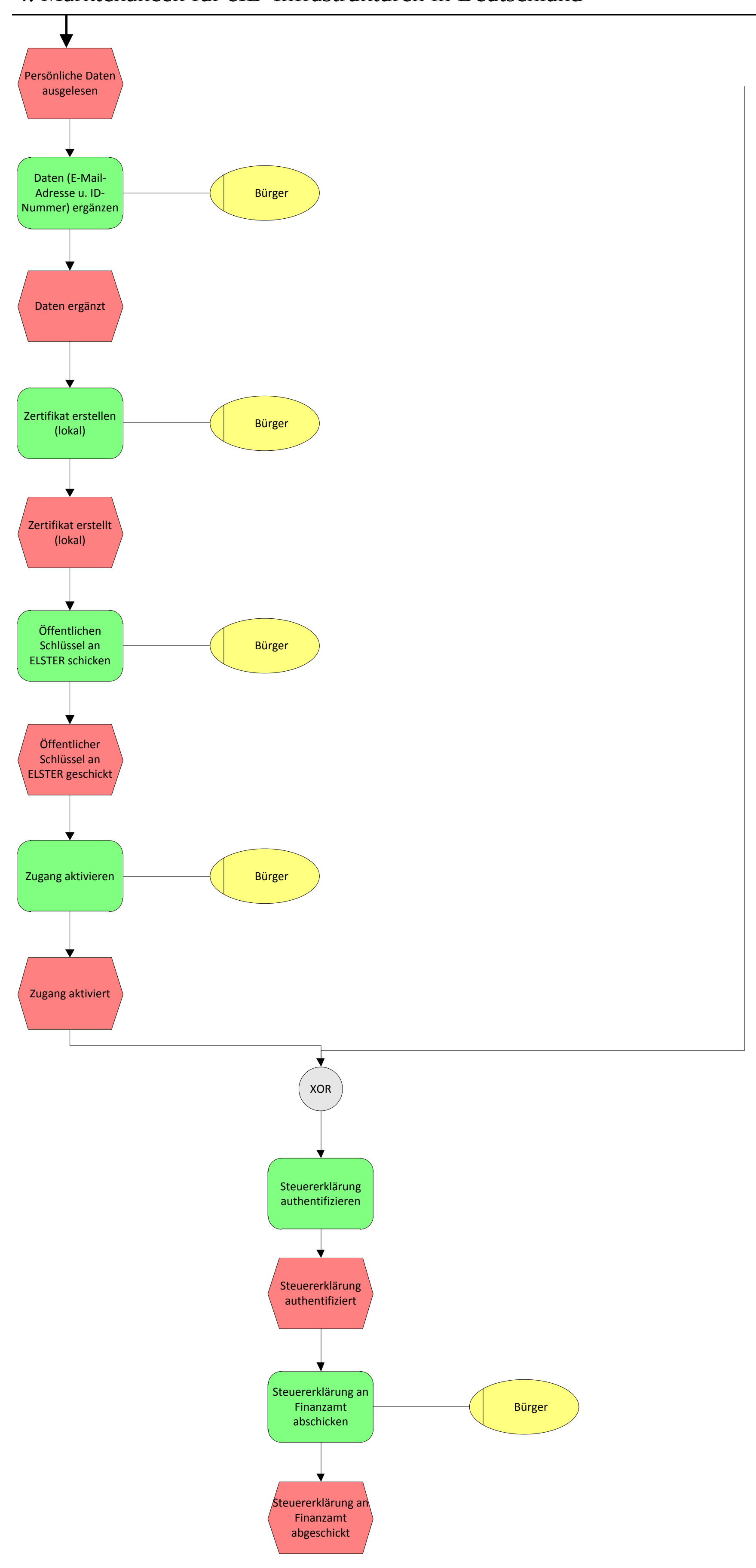


Abbildung 28: EPK ELSTER nach nPA-Einführung (Quelle: Eigene Darstellung)

Ausblick

Die Anzahl der elektronisch eingereichten Steuererklärungen steigt signifikant. Dieses Verfahren spart Ressourcen in den Finanzämtern, schließt Übertragungsfehler (Tippfehler) aus und verringert sowohl den Zeitaufwand für die Eingabe und Bestätigung der Daten seitens der Bürger als auch für die anschließende Bearbeitung der Daten vonseiten der Verwaltung (Bundesministerium des Inneren 2008, 49). Weiter wird durch den Einsatz des nPA ein völlig medienbruchfreier Prozess erreicht (Behörden Spiegel Online 2010). Allerdings sollen die Bürger auch bei dieser Anwendung für die Aktualität der Firewall und des Virenschutzes sorgen, um einen sicheren Datentransfer zu ermöglichen (Borchers 2010c).

4.5.1.3. *Emissionshandel*

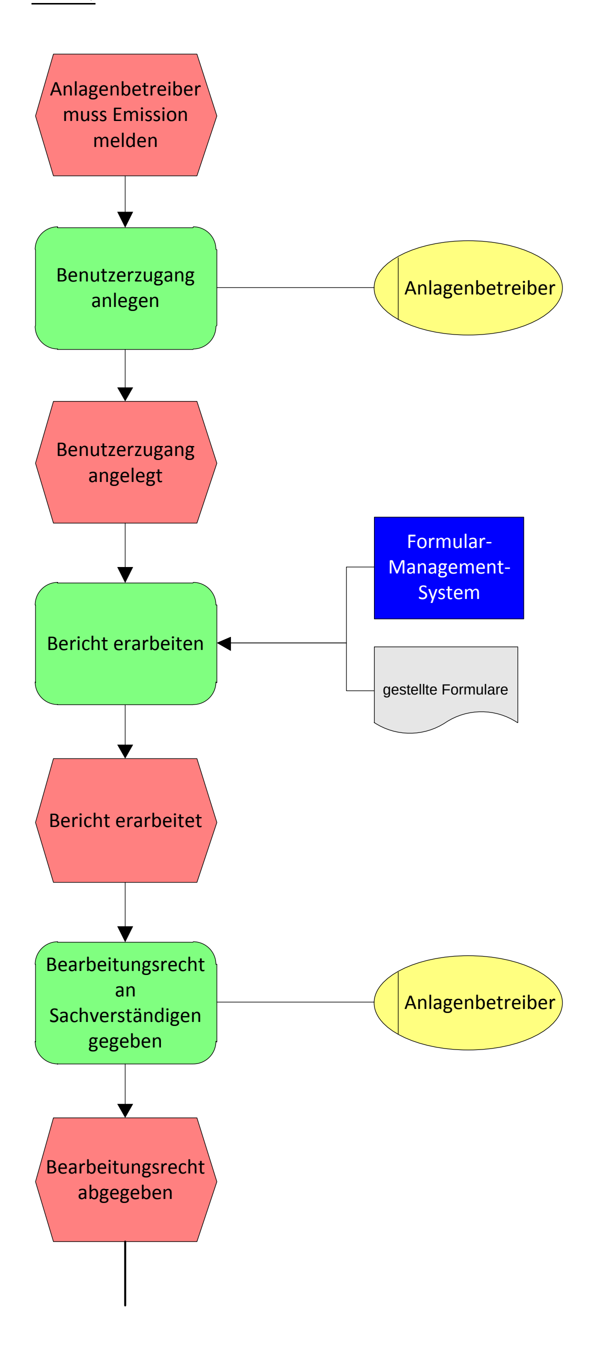
Der Emissionshandel wurde am 01.01.2005 in den Mitgliedsstaaten der Europäischen Union für bestimmte Branchen eingeführt (Umweltbundesamt 2010a). Er basiert auf der für den Umweltschutz grundlegenden Idee zwischen Nutzung von natürlichen Ressourcen und der Verwendung von Geldwerten. Um klimaschädliche Gase ausstoßen zu dürfen, muss man über entsprechende Berechtigungen, repräsentiert durch sogenannte Zertifikate, verfügen. Die gesamte Menge an Zertifikaten ist begrenzt, was zur Reduktion von Treibhausgas-Emissionen führt (Umweltbundesamt 2010a). Die Verwendung solcher Zertifikate durch natürliche und juristische Personen ist entsprechend der EG-Emissionshandelsrichtlinie möglich, wenn sie ein gebührenpflichtiges Handelskonto eröffnen. Die Abwicklung des Handels verwendet Handelsplattformen. Alle Handelskonten werden von der Deutschen Emissionshandelsstelle (DEHSt) geführt, was ein Überblick über die sich im Umlauf befindenden Zertifikate gibt. Zu den Aufgaben von DEHSt zählen dabei unter anderem die Zuteilung von Emissionsberechtigungen, das Kontomanagement der Beteiligten, die Prüfung von Emissionsberichten sowie die nationale und internationale Berichterstattung (Hinz 2006, 3). Wichtige technische Voraussetzung für die elektronische Kommunikation innerhalb von DEHSt ist die Virtuelle Poststelle (VPS) (Hinz 2006, 6). Über diese VPS kommunizieren circa 2.000 Anwender miteinander (o. V. 2009b, 29). Im Folgenden wird die Registrierung und das Installieren der VPS ohne und mit Einsatz des nPA verglichen.

Registrierung und Installation VPS ohne nPA

Aktuell existieren zwei Möglichkeiten sich für die Nutzung der VPS bei der DEHSt zu registrieren. Sollte der Nutzer keine Signaturkarte besitzen, so sind zunächst Formulare zum Identifikationsnachweis sowie zur Bevollmächtigung auszufüllen und an die DEHSt zu senden. Sofern der Nutzer eine Signaturkarte besitzt, entfällt der Identifikationsnachweis gegenüber der DEHSt. Allerdings muss der Nutzer ein Formular zur Nutzung der qualifizierten elektronischen Signatur, mit der er später seine Nachrichten signiert, an die DEHSt schicken (Umweltbundesamt 2010b).

Bei der Installation der VPS wird, ein Zertifikat zur Verschlüsselung der Nachrichten zugewiesen. Es besteht aus einem asymmetrischen Schlüsselpaar mit einem privaten und öffentlichen Schlüssel, um die Sicherheit der Kommunikation zu gewährleisten. Im Anschluss daran und an den Versand der entsprechenden Unterlagen zum Identitätsnachweis prüft die DEHSt die Daten und schaltet das Postfach des neuen Benutzers frei. Erst danach ist die Anmeldung bei der VPS möglich, um die verschiedenen Tätigkeiten im Rahmen des Emissionshandel, wie z. B. die Erstellung von Emissionsberichten und die Zuteilung von Emissionszertifikaten durchzuführen (Deutsche Emissionshandelsstelle im Umweltbundesamt 2010a, 4ff).

<u>EPK:</u>





Daten des Betreibers bestätigen
Sachverständiger
Daten des Betreibers bestätigt
Emissionsbericht erstellen
Emissionsbericht erstellt
Virtuelle Poststelle
Nachricht elektronisch signieren
Sachverständiger
Postfach einrichten mittels papiermäßiger Bearbeitung oder Signaturkarte
Anlagenbetreiber
Nachricht elektronisch signiert
Postfach eingerichtet
Virtuelle Poststelle
Bericht an Anlagenbetreiber übermitteln
Sachverständiger
Bericht an Anlagenbetreiber übermittelt
Virtuelle Poststelle
Qualitätssicherung und gesamte Nach-richt elektronisch signieren
Anlagenbetreiber
QS und gesamte Nachricht elektronisch signiert

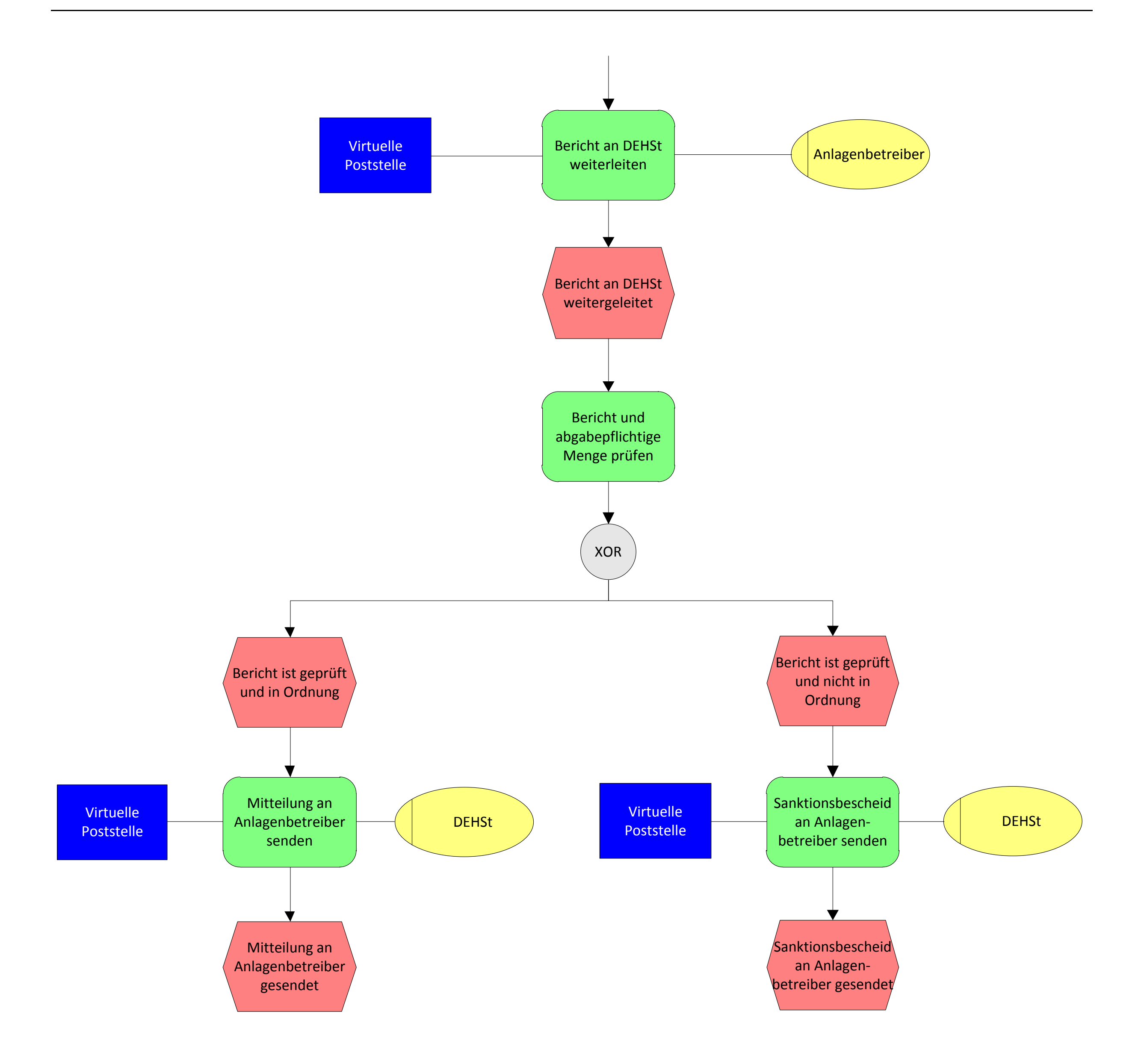


Abbildung 29: EPK Emissionshandel ohne nPA (Quelle: Eigene Darstellung)

Registrierung und Installation VPS mit nPA

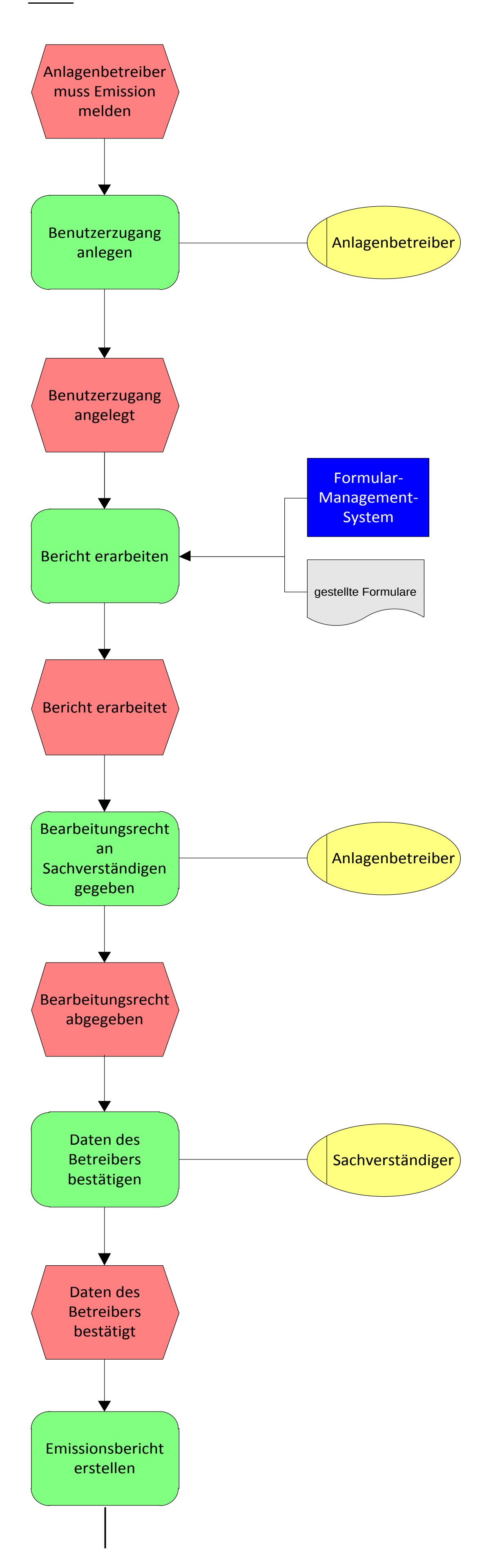
Seit 01.11.2010 bietet DEHSt eine neue Form der Registrierung an, die das bisherige Versenden einer Kopie des Personalausweises durch den Einsatz des nPA ersetzt (Umweltbundesamt 2010d, 15). Die Kommunikation zwischen Benutzer und DEHSt und die gegenseitige Authentisierung läuft über ein Applet ab, das über eine Internetseite zu starten (Umweltbundesamt 2010d, 15) und somit plattform-unabhängig ist (o. V. 2009b, 29). Der eID-Server wird kontaktiert und führt eine gegenseitige Authentisierung durch (Umweltbundesamt 2010d, 15). Sobald der Benutzer seine Daten eingegeben, bestätigt und abgeschickt hat, kann die Registrierung abgeschlossen und die Anwendung DEHSt-VPSMail heruntergeladen und ausgeführt werden. Alle Funktionen der Anwendung werden sofort freigeschaltet (Umweltbundesamt 2010d, 20). Die qualifizierte elektronische Signatur des nPA wird

zur Bestätigung der Transaktionen verwendet und löst die Verwendung von Passwörtern ab (o. V. 2009b, 29) (vgl. Abbildung 30).

Zuteilung von Emissionszertifikaten

Nachdem Benutzer sich für den Emissionshandel bei der DEHSt registriert hat und berechtigt ist, VPS zu nutzen, hat er die Möglichkeit einen Zuteilungsantrag für Emissionszertifikate an die DEHSt zu stellen. Zunächst füllt der Betreiber dazu Online im FMS (Formular Management System) das Zuteilungsformular aus, welches im Anschluss daran von einem Sachverständigen verifiziert wird. Der Sachverständige erstellt den fertigen Zuteilungsantrag als ZIP-Datei und erstellt in der VPS eine Nachricht mit dem Zuteilungsantrag im Anhang. Zum Versand wird der öffentliche Schlüssel des Empfängers angefordert und die Nachricht zunächst mit diesem verschlüsselt. Anschließend wird die Nachricht nach dem OSCI-Prinzip vom Intermediär, in dem Fall die VPS, ein zweites Mal für Transportzwecke verschlüsselt und versandt. Der Intermediär übernimmt sowohl eine Überprüfung des öffentlichen Schlüssels als auch das Erstellen eines Zeitstempels für die Nachricht. Der fertige und an den Betreiber zurückgeschickte Zuteilungsantrag wird mit seinem privaten Schlüssel entschlüsselt, um den Inhalt lesbar zu machen. Anschließend ist der Antrag vom Betreiber an die DEHSt zu senden. Dazu wird das Verfahren nach dem OSCI-Prinzip wiederholt. Von Bedeutung an dieser Stelle ist, dass die Verschlüsselung sowohl mittels des selbst erzeugten asymmetrischen Schlüsselpaars, als auch mit der qualifizierten elektronischen Signatur, die für den neuen Personalausweis beschafft werden kann, funktioniert. Die DEHSt errechnet im Anschluss an den Erhalt des Antrags die Zuteilungsmenge an Emissionszertifikaten, erstellt den Zuteilungsbescheid und versendet ihn über die VPS an den Betreiber (Hinz 2006).

EPK


Anlagenbetreiber muss Emission melden
Benutzerzugang anlegen
Anlagenbetreiber
Benutzerzugang angelegt
Formular-Management-System
Bericht erarbeiten
gestellte Formulare
Bericht erarbeitet
Bearbeitungsrecht an Sachverständigen gegeben
Anlagenbetreiber
Bearbeitungsrecht abgegeben
Daten des Betreibers bestätigen
Sachverständiger
Daten des Betreibers bestätigt
Emissionsbericht erstellen


Emissionsbericht erstellt
Virtuelle Poststelle
Nachricht elektronisch signieren
Sachverständiger
Postfach einrichten mittels nPA
Anlagenbetreiber
Nachricht elektronisch signiert
Postfach eingerichtet
Virtuelle Poststelle
Bericht an Anlagenbetreiber übermitteln
Sachverständiger
Bericht an Anlagenbetreiber übermittelt
Virtuelle Poststelle
Qualitätssicherung und gesamte Nachricht elektronisch signieren
Anlagenbetreiber
QS und gesamte Nachricht elektronisch signiert
Virtuelle Poststelle
Bericht an DEHSt weiterleiten
Anlagenbetreiber
Bericht an DEHSt weitergeleitet

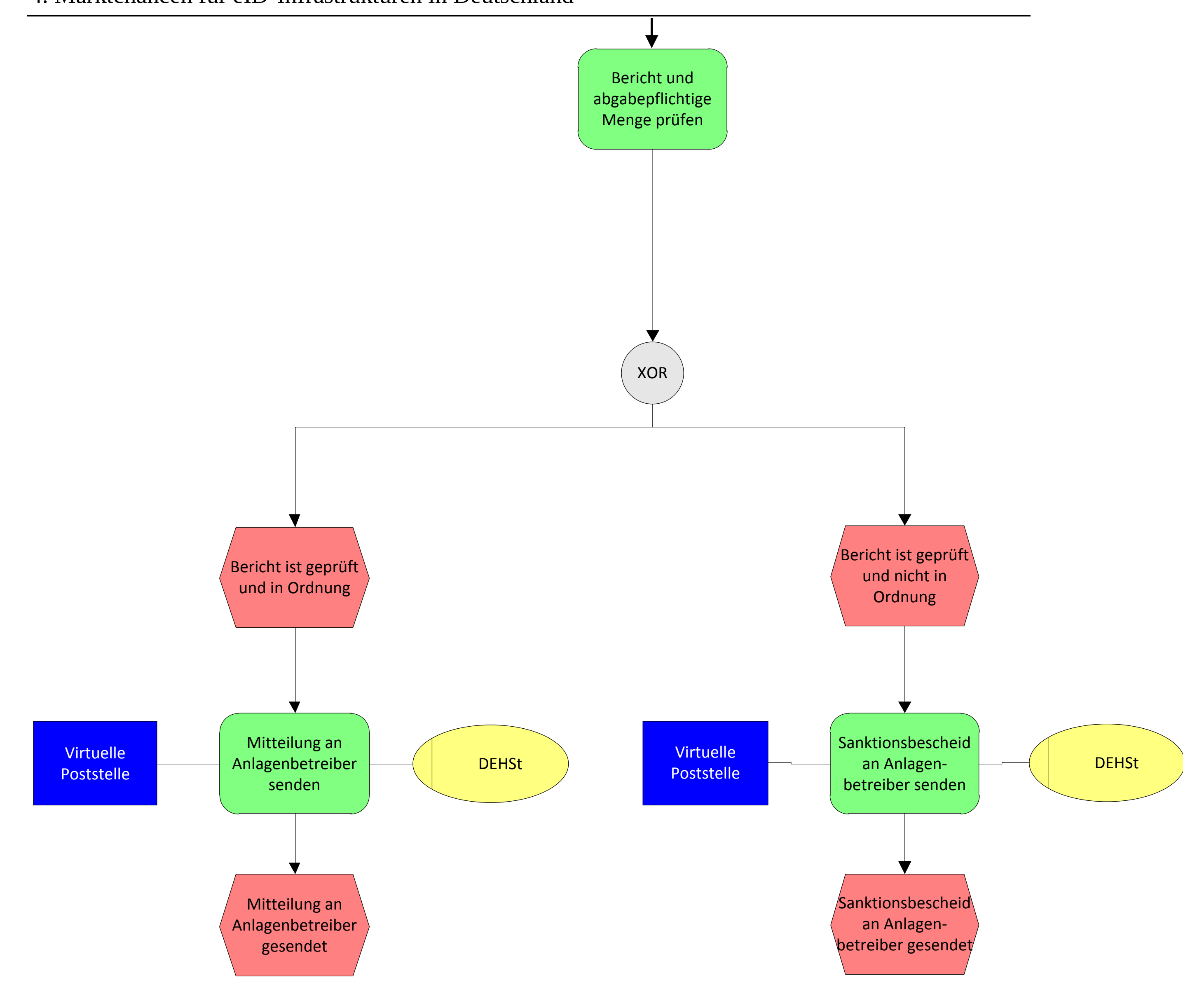


Abbildung 30: EPK Emissionshandel nach nPA-Einführung

Eine weitere Möglichkeit, die online genutzt werden kann, ist die Emissionsberichterstattung. Ein zweiter wesentlicher Punkt beim Emissionshandel ist die Emissionsberichterstattung, die jährlich zum 01.03. eines Jahres für das vorangegangene Jahr durch den Anlagenbetreiber vorzunehmen ist. Hier wird zunächst durch den Betreiber im FMS ein entsprechender Bericht erfasst, der zunächst von einem Sachverständigen geprüft wird. Im Anschluss daran trägt der Sachverständige die Emissionsdaten des Betreiber in das Register der DEHSt ein und erstellt in der VPS eine entsprechende Nachricht für Emissionsberichte, die wieder mit den zuvor beschriebenen möglichen Verfahren des selbst erstellten Verschlüsselungszertifikats oder der qualifizierten elektronischen Signatur verschlüsselt wird. Der Betreiber erstellt im Anschluss über die VPS eine Nachricht mit dem fertigen Emissionsbericht und sendet diese an die zuständige Landesbehörde, die den Bericht prüft und ihrerseits über die VPS an die DEHSt weiterleitet. Diese verwaltet die Emissionsberichte und setzt mit der Emissionsberichterstattung die gesetzlichen Vorgaben zum Klimaschutz um (Umweltbundesamt 2010c).

Ausblick

Die Analyse der Verfahren im Rahmen des Emissionshandels, die durch die DEHSt umgesetzt wurden, zeigt, dass Prozesse wie die Zuteilung von Emissionszertifikaten und die Emissionsberichterstattung benutzerfreundlicher und medienbruchfrei umgesetzt werden. Ein wesentlicher Nachteil des klassischen Verfahrens war die umständliche, zeitintensive und nicht medienbruchfreie Registrierung zur Teilnahme am Emissionshandel und zur Nutzung der VPS. Bisher musste jeder Benutzer, der sich registrieren möchte, Formulare ausfüllen und in Papierform mit einer Kopie des Personalausweises an die DEHSt postalisch versenden. Durch die Einführung des neuen Personalausweises kann an dieser Stelle die eID-Funktion des nPA genutzt werden, um den Vorgang zu modernisieren und zu verbessern. Damit wird die Registrierung wesentlich vereinfacht, medienbruchfrei und weniger zeitintensiv. Der neue Personalausweis hat positiven Einfluss auf die Verfahren des Emissionshandels und wird die Kosten für die Kommunikation in Papierform reduzieren.

4.5.1.4. *Gewerbeanmeldung*

Wer in Deutschland in die Selbstständigkeit gehen möchte oder aber bestimmte Nebentätigkeiten ausüben will, muss eine administrative Hürde überwinden – die Gewerbeanmeldung. Im Jahr 2009 wurden 864.415 Gewerbe angemeldet (Statistisches Bundesamt Deutschland 2009b) und 728.318 Gewerbe abgemeldet (Statistisches Bundesamt Deutschland 2009a). Die Vielzahl dieser Vorgänge muss von den kommunalen Behörden bearbeitet werden und das keinesfalls in überwiegend elektronischer Form. So hat das Frauenhofer ISI 2004 in einer Erhebung im Bundesland Baden-Württemberg ermittelt, dass in nur 46 % der Kommunen des Landes die Gewerbeanmeldung als E-Government-Angebot bereitgestellt wurde (Kimpeler et al. 2005, 2). Konkret bedeutet das, dass in vielen Kommunen in Deutschland die Gewerbeanmeldung nach wie vor nur in Papierform und teilweise elektronisch, im Rahmen des E-Government in Kombination mit Nachweisverfahren in Papierform, möglich ist. Zukünftig erhofft man sich durch den Einsatz des neuen Personalausweises das Verfahren zur Gewerbeanmeldung vollständig elektronisch abwickeln zu können.

Gewerbeanmeldung ohne nPA

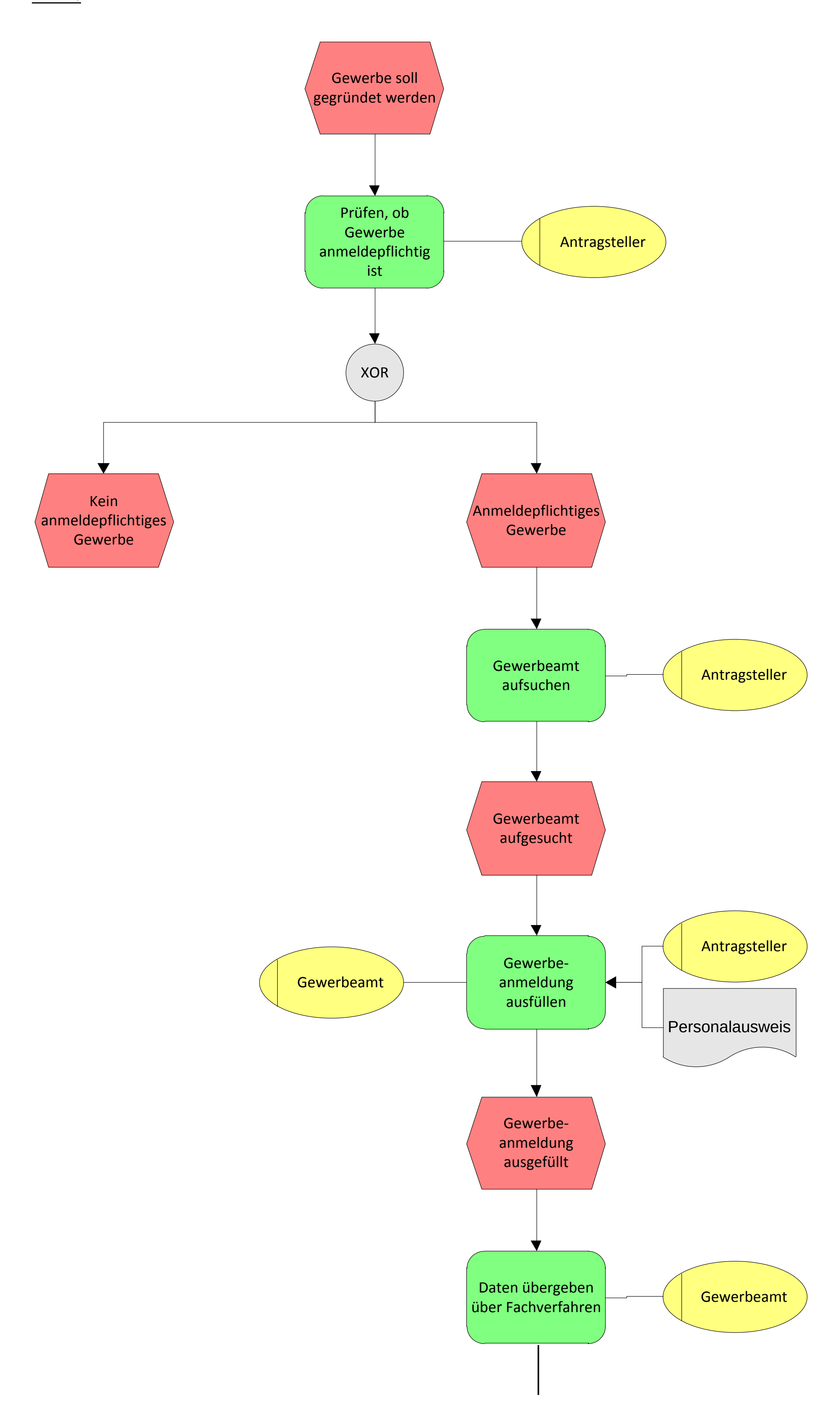
Die Gewerbeanmeldung erfolgt derzeit entweder vollständig in Papierform oder aber teilweise online (DIHK 2009, 13). Voraussetzungen für die Gewerbeanmeldung sind unter anderem ein getätigter Eintrag in das Handelsregister sowie ein Nachweis der Identität (DIHK 2009, 6). Studien und Umfragen zeigten, dass die Mehrheit der Gewerbeanmeldungen ein zeitaufwendiger Prozess ist, der mit lange Wartezeiten und mehrfachem Ausfüllen und Verschicken von Formulare verbunden ist (DIHK 2009, 12). Um sein Gewerbe anmelden zu können, muss der Antragsteller seine Identität nachweisen. Es existieren folgende Möglichkeiten zur Gewerbeanmeldung: persönlich vor Ort bei der Behörde, postalisch und, in seltenen Fälle, teilweise internetgestützte Anmeldung. Allerdings werden Personaldoku-

menten (Personalausweis oder Reisepass und Meldebestätigung) sowie weitere Dokumente (in Abhängigkeit von der Staatsangehörigkeit und Art der Unternehmung) in Fotokopie zu übermitteln (DIHK 2009, 13). Des Weiteren müssen regionale Unterschiede beim Verfahren berücksichtigt werden (DIHK 2009, 13). Durch diesen Medienbruch entstehen unnötige Aufwände für den Antragsteller, aber auch für die Behörden (DIHK 2009, 13).

Die Gewerbeanmeldung erfolgt derzeit bei der Gemeinde, in der das Gewerbe angemeldet werden soll. Dabei ist vor Ort im Bürgerbüro der Personalausweis oder Reisepass des Anmeldenden vorzulegen, um die Personalien überprüfen zu können. Bei Handels-, Vereins- oder Genossenschaftsregister eingetragene Firmen ist ebenfalls der Registerauszug vorzulegen. Bei der Gründung einer GmbH ist eine Abschrift des notariellen Gründungsvertrages sowie eine Vollmacht der Gründer, wonach der Gewerbebeginn bereits vor der Handelsregistereintragung aufgenommen werden soll vorzuzeigen. Anschließend bescheinigt die Behörden den Empfang der Gewerbeanzeige (sog. Gewerbeschein). Des Weiteren werden von der Behörde Finanzamt, Registergericht, Landesverband der Berufsgenossenschaften, Statistisches Landesamt sowie das Arbeitsamt verständigt (München.de 2010).

Eine weitere Möglichkeit, derzeit ein Gewerbe online anzumelden, ist die Anwendung KoGeMa der Datenzentrale Baden-Würrtemberg (DZBW). Die Anwendung KoGeMa ist eine integrierte Gesamtlösung zur Unterstützung des gesamten Vorgangs der Gewerbeanmeldung. Dabei wird eine Online-Antragstellung, die elektronische Bearbeitung des Antrags durch den Sachbearbeiter sowie nachgelagerte Tätigkeiten wie die Erstellung des Bescheids, die Erteilung von Auskünften und statistische Auswertungen ermöglicht. Der Antragsteller füllt im ersten Schritt online den Antrag aus. Anschließend wird der Antrag vom Antragsteller elektronisch gesendet und über eine SSL-verschlüsselte Verbindung übertragen. Zeitgleich muss der Anwender jedoch in Papierform den Identitätsnachweis erbringen, im Fall von KoGeMa bedeutet das, dass eine Kopie des Personalausweises und eine Unterschrift des Antragsteller dem Sachbearbeiter schriftlich zugesandt werden müssen. Bei alternativen Lösungen ist auch eine qualifizierte elektronische Signatur des Online-Antrags möglich, die jedoch nicht vom Nachweis der Identität mittels Personalausweis entbindet. Im Anschluss daran prüft der Sachbearbeiter den Antrag und kann nach erfolgreicher Prüfung den Bescheid erstellen und versenden. Weiterhin können Sachbearbeiter dank der zentralen Datenbank von KoGeMa Auskünfte erteilen, Auswertungen erstellen und die gesetzlich vorgesehen Datenübermittlung per Papier oder online vornehmen (Datenzentrale Baden-Württemberg o. J.) (vgl. Abbildung 31).

EPK:


Gewerbe soll gegründet werden
Prüfen, ob Gewerbe anmeldepflichtig ist
Antragsteller
XOR
Kein anmeldepflichtiges Gewerbe
Anmeldepflichtiges Gewerbe
Gewerbeamt aufsuchen
Antragsteller
Gewerbeamt aufgesucht
Gewerbeamt
Gewerbe-anmeldung ausfüllen
Antragsteller
Personalausweis
Gewerbe-anmeldung ausgefüllt
Daten übergeben über Fachverfahren
Gewerbeamt

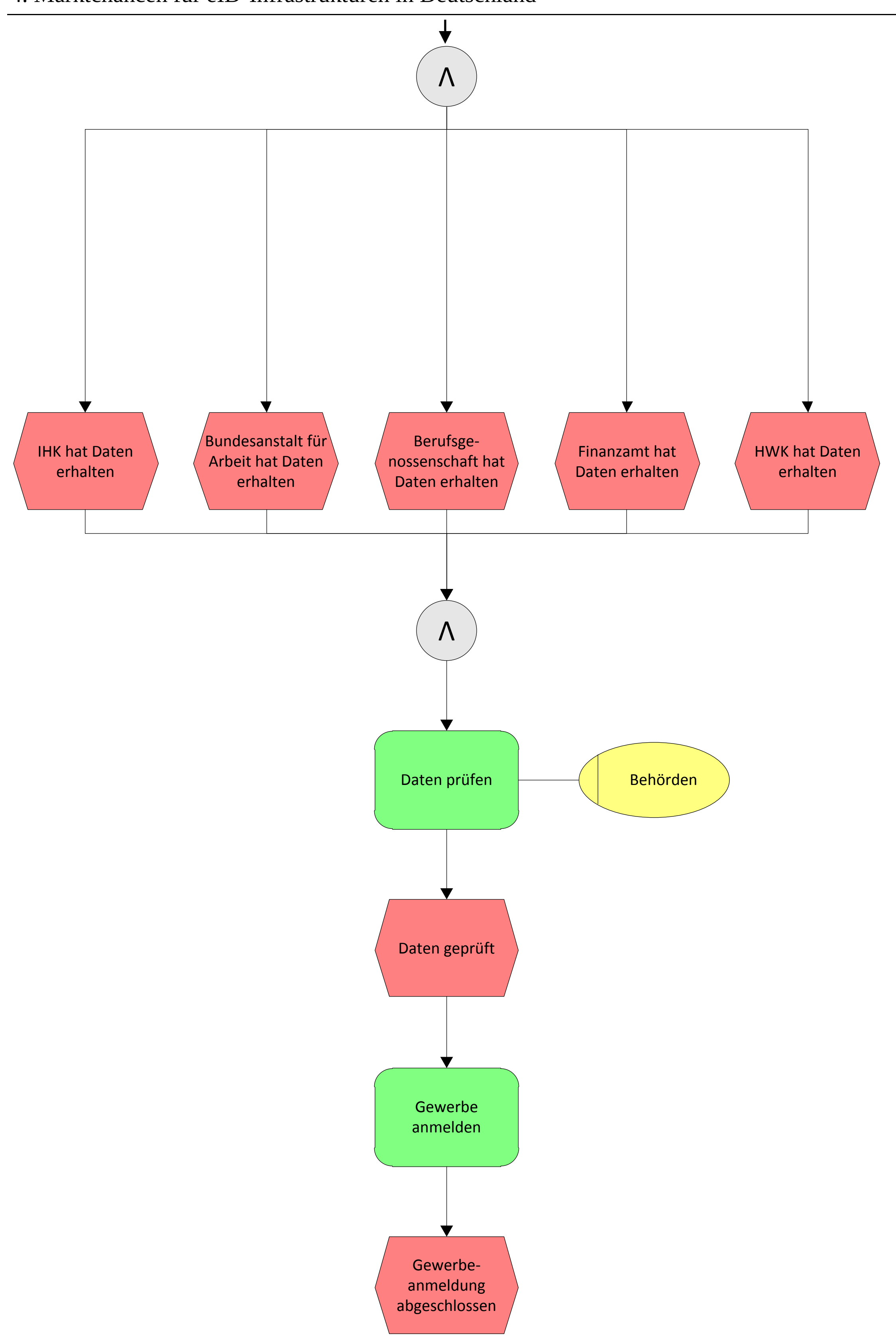
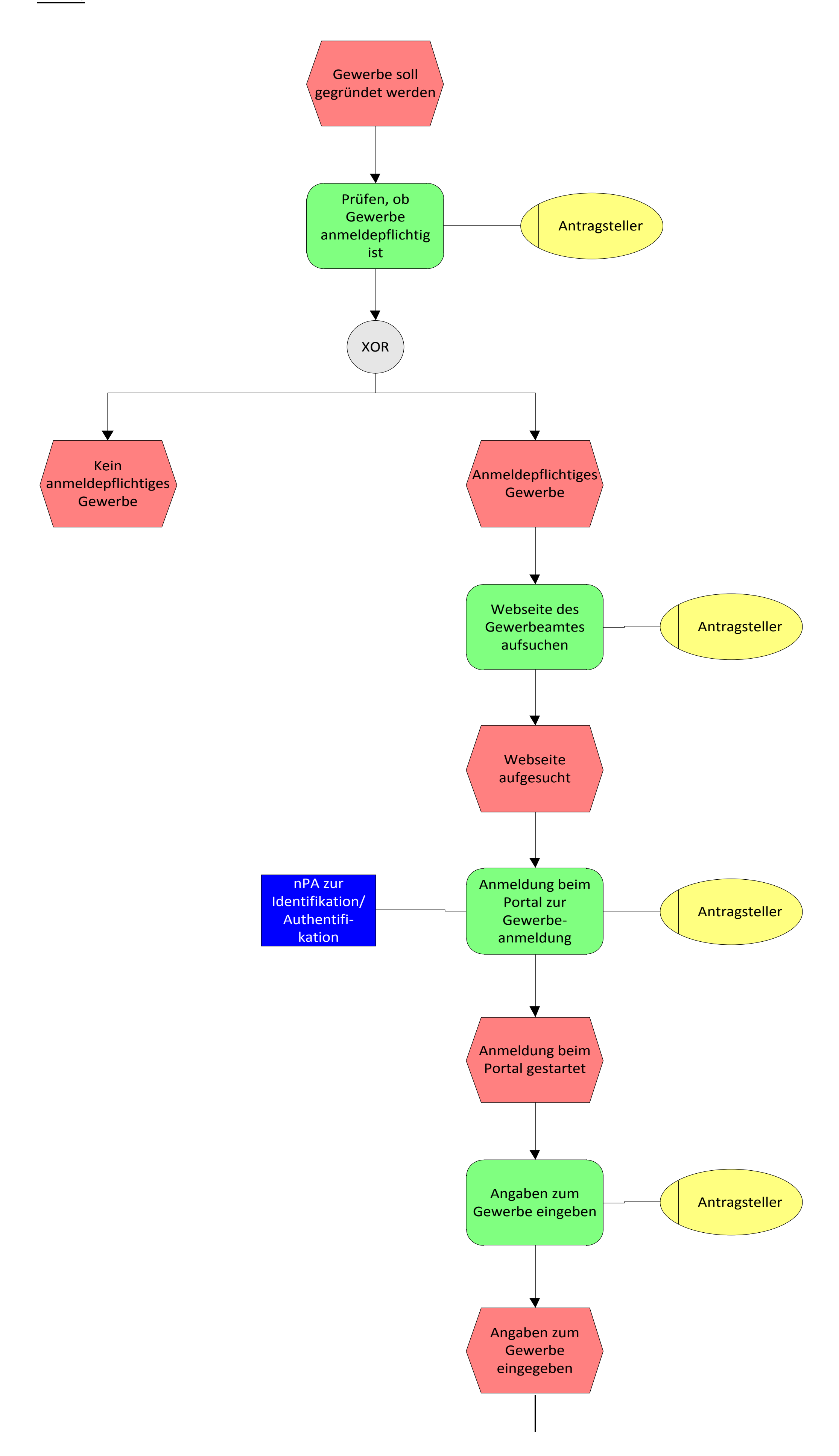


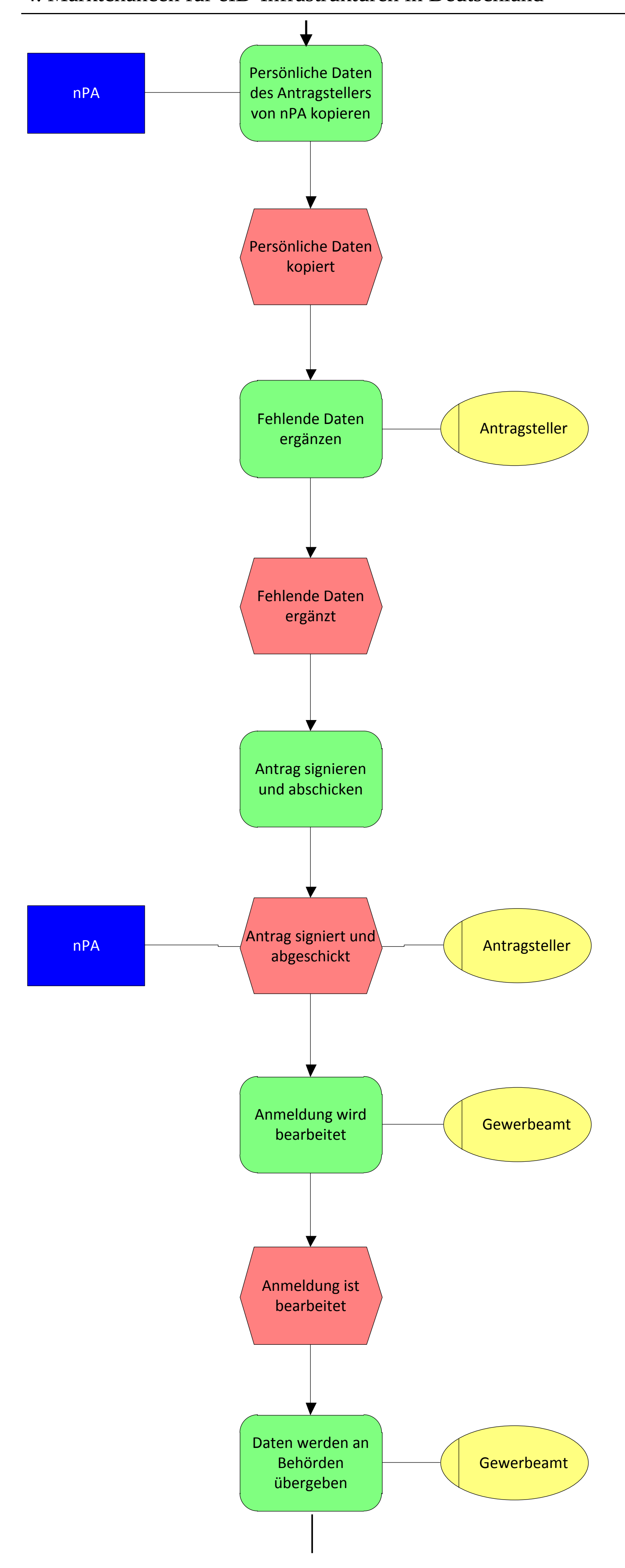
Abbildung 31: EPK vor nPA-Einführung (Quelle: Eigene Darstellung)

Gewerbeanmeldung nach nPA

Mit der Einführung des neuen Personalausweises soll die eID-Funktion des nPA genutzt, um die bisherige Papierform des Identitätsnachweises zu ersetzen (Datenzentrale Baden-Württenmberg 2010, 23). Es soll der Prototyp aus dem Anwendungstest weiterentwickelt werden (Datenzentrale Baden-Württenmberg 2010, 23), um ein einheitliches staatlich geregeltes System zu entwerfen (Datenzentrale Baden-Württenmberg 2010, 4), in dem aber individuelle Einstellungen für jede Kommune ermöglicht werden (Datenzentrale Baden-Württenmberg 2010, 23). Die Umsetzung erfolgt durch die Integration der AusweisApp in die Anwendung KoGeMa (Datenzentrale Baden-Württemberg o. J.). Der Prozess der Gewerbeanmeldung beginnt, indem sich der Antragsteller und die Gewerbebehörde über einen eID-Server authentisieren. Dabei hat die Gewerbebehörde ein entsprechendes Berechtigungszertifikat zum Auslesen der Daten des neuen Personalausweises des Antragstellers. Sobald der eID-Service Provider Antragsteller und Gewerbebehörde authentifiziert hat, kann die Gewerbebehörde die Daten des Antragstellers vom neuen Personalausweis auslesen. Parallel dazu kann der Antragsteller den Online-Antrag zur Gewerbeanmeldung bereits ausfüllen und im Anschluss an die Erbringung des Identitätsnachweises mittels eID, absenden. Es ist weiterhin möglich, eine qualifizierte elektronische Signatur zu erwerben und auf dem neuen Personalausweis zu speichern, um z. B. für andere Anwendungen zur Gewerbeanmeldung eine gegebenenfalls nötige elektronische Unterschrift zu leisten. Sobald der Antrag zur Gewerbeanmeldung im System KoGeMa nun bei der Gewerbebehörde eingeht, kann der Sachbearbeiter den Antrag prüfen und den Bescheid elektronisch zurücksenden (vgl. Abbildung 32) (Datenzentrale Baden-Württenmberg 2010, 5).

EPK:


Gewerbe soll gegründet werden
Prüfen, ob Gewerbe anmeldepflichtig ist
Antragsteller
XOR
Kein anmeldepflichtiges Gewerbe
Anmeldepflichtiges Gewerbe
Webseite des Gewerbeamtes aufsuchen
Antragsteller
Webseite aufgesucht
nPA zur Identifikation/ Authentifi-kation
Anmeldung beim Portal zur Gewerbe-anmeldung
Antragsteller
Anmeldung beim Portal gestartet
Angaben zum Gewerbe eingeben
Antragsteller
Angaben zum Gewerbe eingegeben


nPA
Persönliche Daten des Antragstellers von nPA kopieren
Persönliche Daten kopiert
Fehlende Daten ergänzen
Antragsteller
Fehlende Daten ergänzt
Antrag signieren und abschicken
nPA
Antrag signiert und abgeschickt
Antragsteller
Anmeldung wird bearbeitet
Gewerbeamt
Anmeldung ist bearbeitet
Daten werden an Behörden übergeben
Gewerbeamt

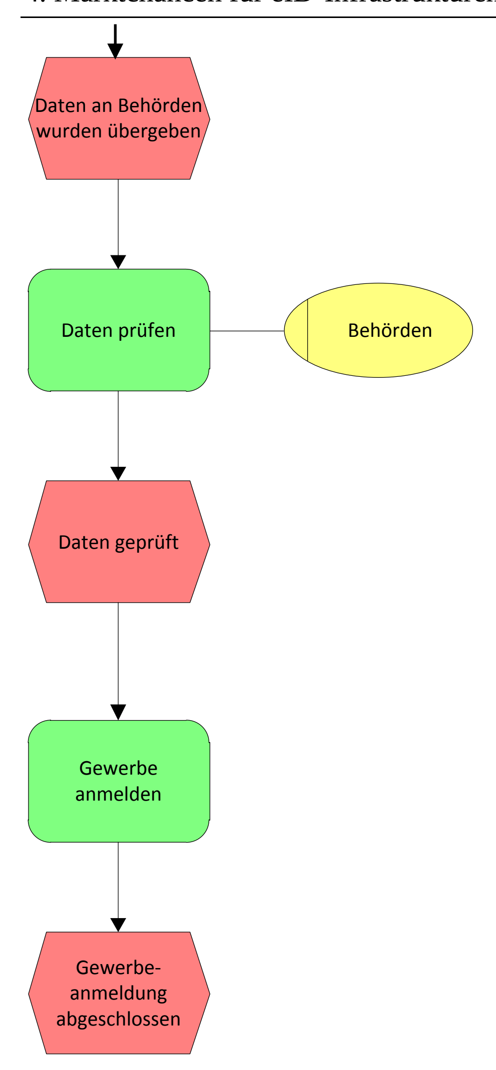


Abbildung 32: EPK Gewerbeanmeldung nach nPA-Einführung (Quelle: Eigene Darstellung)

Der Antragssteller prüft, ob sein Gewerbe anmeldungspflichtig ist. Falls dies der Fall ist, sucht er die Webseite des Gewerbeamts auf und startet das Portal zur Gewerbeanmeldung. Hierfür benötigt er den nPA zur Identifikation und Authentifikation sowie den Bürgerclient. Er macht Angaben zum Gewerbe, wie z. B. Rechtsform und Art des Betriebes. Die persönlichen Daten des Antragsstellers, die auf dem nPA gespeichert sind, werden in den Dialog übernommen, fehlende persönliche Daten werden ergänzt. Als letzten Schritt signiert er den Antrag mithilfe des nPA und schickt ihn an das Gewerbeamt. Im Anschluss daran wird der Antrag von Mitarbeitern des Gewerbeamtes bearbeitet und an weitere Behörden/Institutionen (z. B. Finanzamt, IHK) übergeben. Daten werden von Behörden/Institutionen geprüft und anschließend ist das Gewerbe angemeldet. Der Gewerbeschein wird entweder dann per Post an den Antragsteller gesandt oder vom Antragsteller vor Ort im Bürgerbüro abgeholt.

Mit der Nutzung des neuen Personalausweises bei der Gewerbeanmeldung ist zwar die Antragstellung vollständig elektronisch und daher schneller und einfach, der Gewerbeschein wird aber dennoch weiterhin in Papierform ausgehändigt. Nach Einschätzungen des Interviewpartners wird weiterhin überwiegend die persönliche Gewerbeanmeldung im Bürgerbüro durch den Antragsteller vorgenommen

werden, da durch diesen Prozess der Gewerbeschein gleich ausgehändigt wird dadurch eine zeitliche Ersparnis für den Antragsteller entsteht.

Der Gewerbetreibende soll sich mit dem nPA in der zentralen Benutzerverwaltung registrieren können. Dann kann die Gewerbeanmeldung vollständig elektronisch vorgehen. Die Daten aus seinem Benutzerprofil sind somit zuverlässig und können in der Anwendung übernommen werden (KoopA 2010, I-9).Weiter erlaubt diese Modernisierung vom Prozess die medienbruchfreie Arbeit zwischen Behörden und Institutionen.

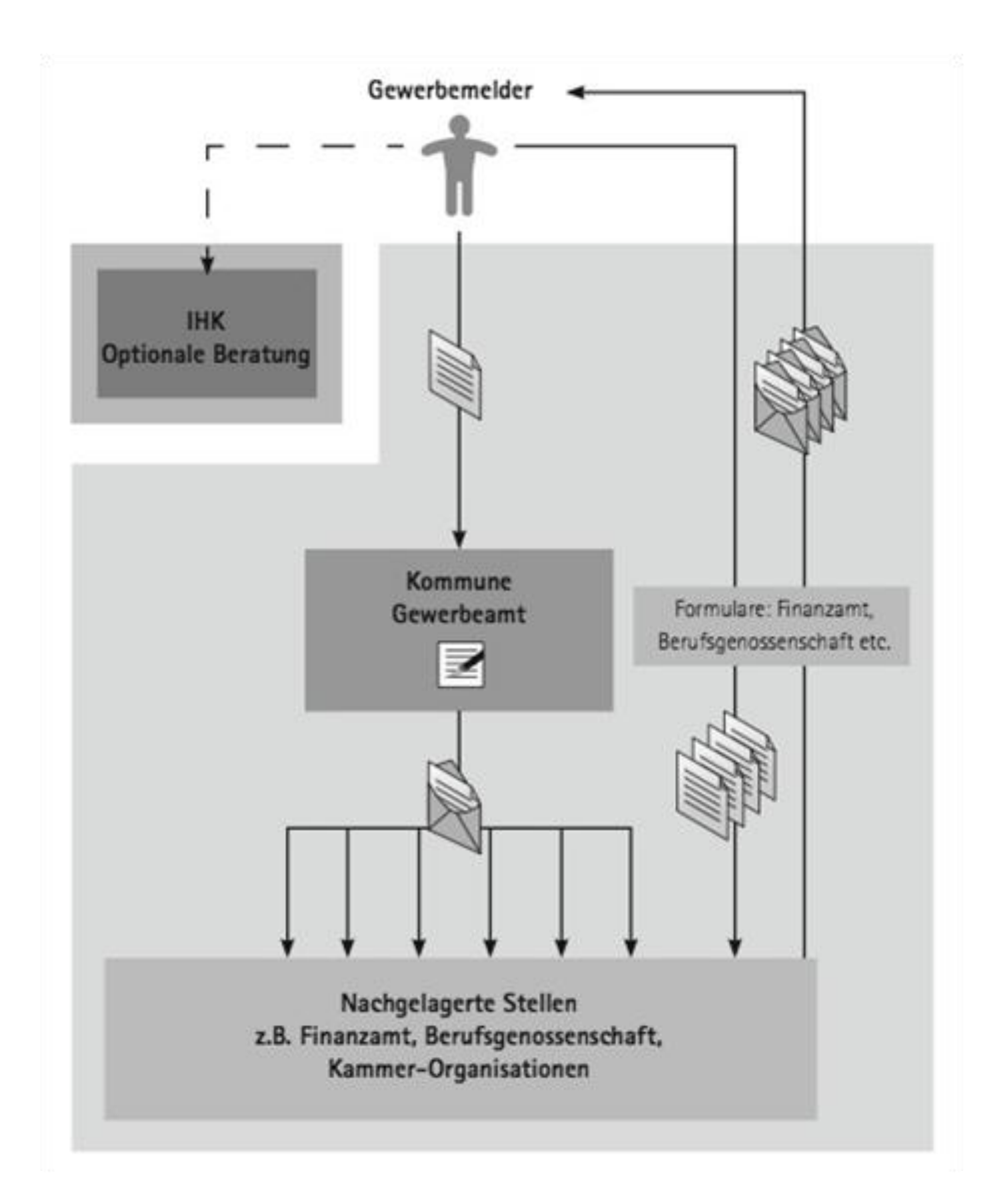


Abbildung 33: Gewerbeanmeldung ohne nPA (Quelle: In Anlehnung an (DIHK 2009, 12)

<u>Ausblick</u>

Der Einsatz des nPA für die Gewerbeanmeldung soll nicht nur das Ziel verfolgen, diese für den Gewerbetreibenden attraktiver anzubieten, sondern soll auch dadurch eine verwaltungsintern schnellere und komfortablere Antragsbearbeitung bieten.

4.5.1.5. *Gesamtauskunft*

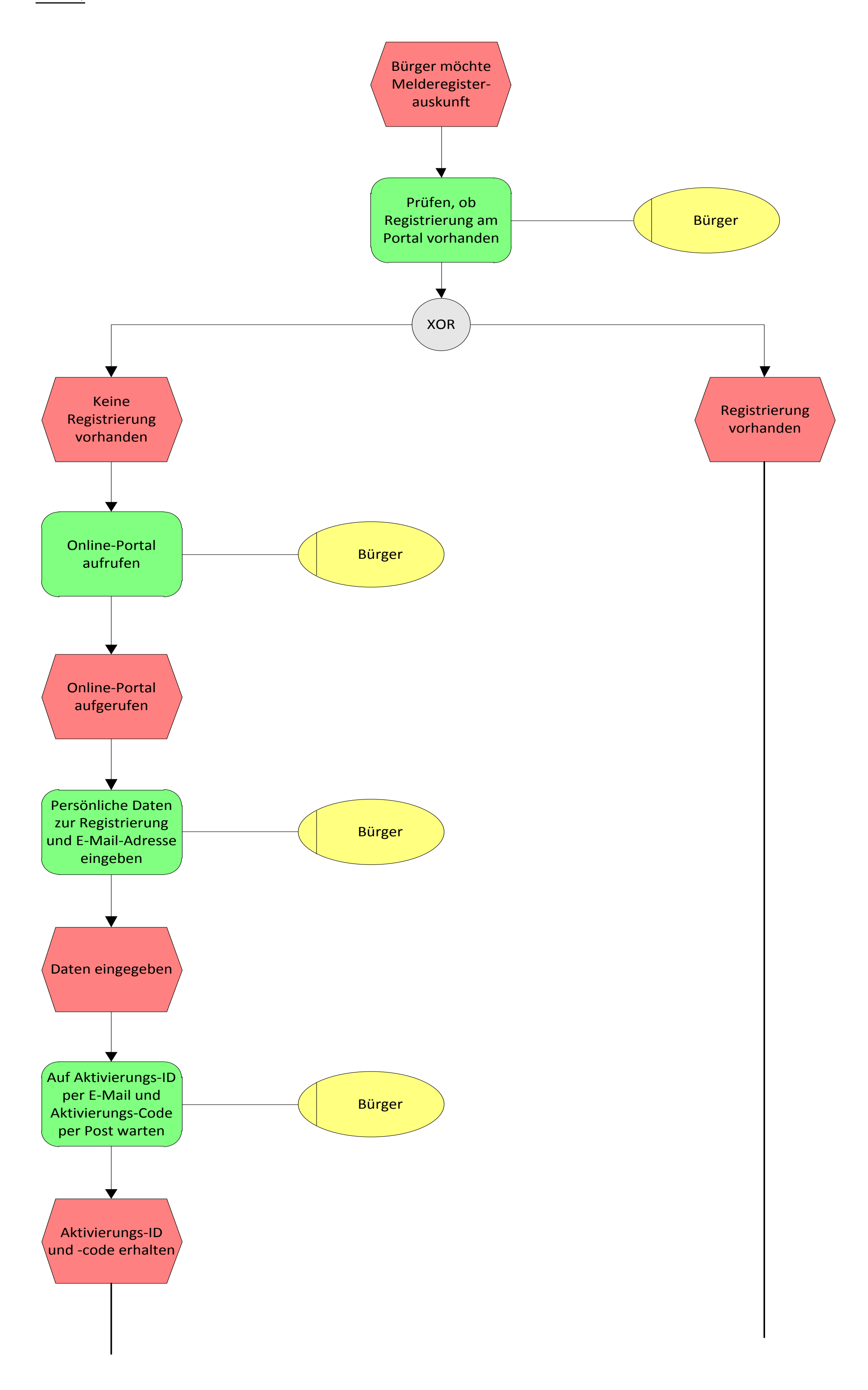
In Deutschland haben die Meldebehörden die Aufgabe, die in ihrem Einflussbereich lebenden Bürger zu registrieren und zu erfassen, um deren Identität und Wohnsitz feststellen zu können. Zu den gespeicherten Daten gehören nach dem Melderechtsrahmengesetz (MRRG)[7] u. a. Name, Geburtstag und -ort, akademischer Titel sowie Anschrift und Angaben zu weiteren Familienangehörigen. Nach § 8 MRRG hat die Behörde einem Bürger auf Anfrage alle über ihn gespeicherten Daten mitzuteilen (Bundesministerium der Justiz 2010b). Diesen Vorgang nennt man auch Gesamtauskunft. Zusätzlich haben Dritte die Möglichkeit eine einfache bzw. erweiterte Auskunft über eine Person einzuholen. Diese kostenpflichtige Dienstleistung enthält entweder nur den vollständigen Namen, Doktorgrad und Anschriften eines bestimmten Bürgers, bei glaubhaft machen eines berechtigten Interesses zusätzlich noch einige weitere Informationen (o. V. 2010a).

<u>Gesamtauskunft ohne nPA</u>

Bisher können nur die einfache bzw. erweiterte Auskunft online eingeholt werden, meist mithilfe eines Intermediärs wie z. B. ZEMA (www.zemaonline.de). Laut Gesetz ist auch eine Erteilung der Gesamtauskunft automatisiert über das Internet möglich, sofern entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden (Bundesministerium der Justiz 2010b). Faktisch gibt es jedoch keine Behörde, die diesen Service derzeit anbietet, daher muss ein Betroffener den Antrag persönlich oder schriftlich stellen und bekommt das Dokument normalerweise per Post. Hierbei muss je nach Bundesland ein Formular ausgefüllt (entfällt meist bei persönlicher Einholung) und eine Gebühr von etwa 5€ – je nach Behörde – entrichtet werden.

[7] Melderechtsrahmengesetz in der Fassung der Bekanntmachung vom 19. April 2002 (BGBl. I S. 1342), das zuletzt durch Artikel 3 des Gesetzes vom 18. Juni 2009 (BGBl. I S. 1346) geändert worden ist.

EPK:


Bürger möchte Melderegister-auskunft
Prüfen, ob Registrierung am Portal vorhanden
Bürger
XOR
Keine Registrierung vorhanden
Registrierung vorhanden
Online-Portal aufrufen
Bürger
Online-Portal aufgerufen
Persönliche Daten zur Registrierung und E-Mail-Adresse eingeben
Bürger
Daten eingegeben
Auf Aktivierungs-ID per E-Mail und Aktivierungs-Code per Post warten
Bürger
Aktivierungs-ID und -code erhalten

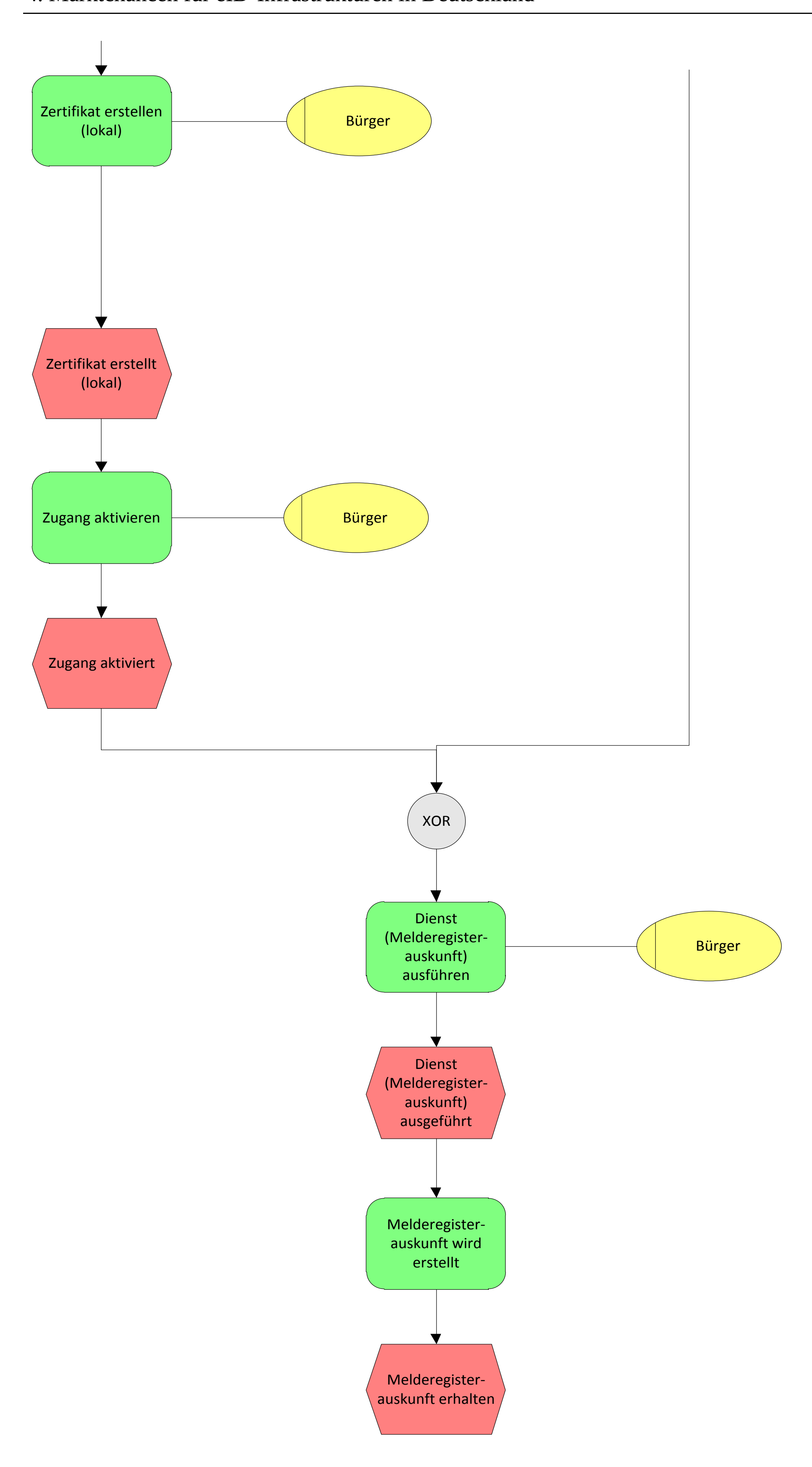


Abbildung 34: EPK Gesamtauskunft vor nPA-Einführung (Quelle: Eigene Darstellung)

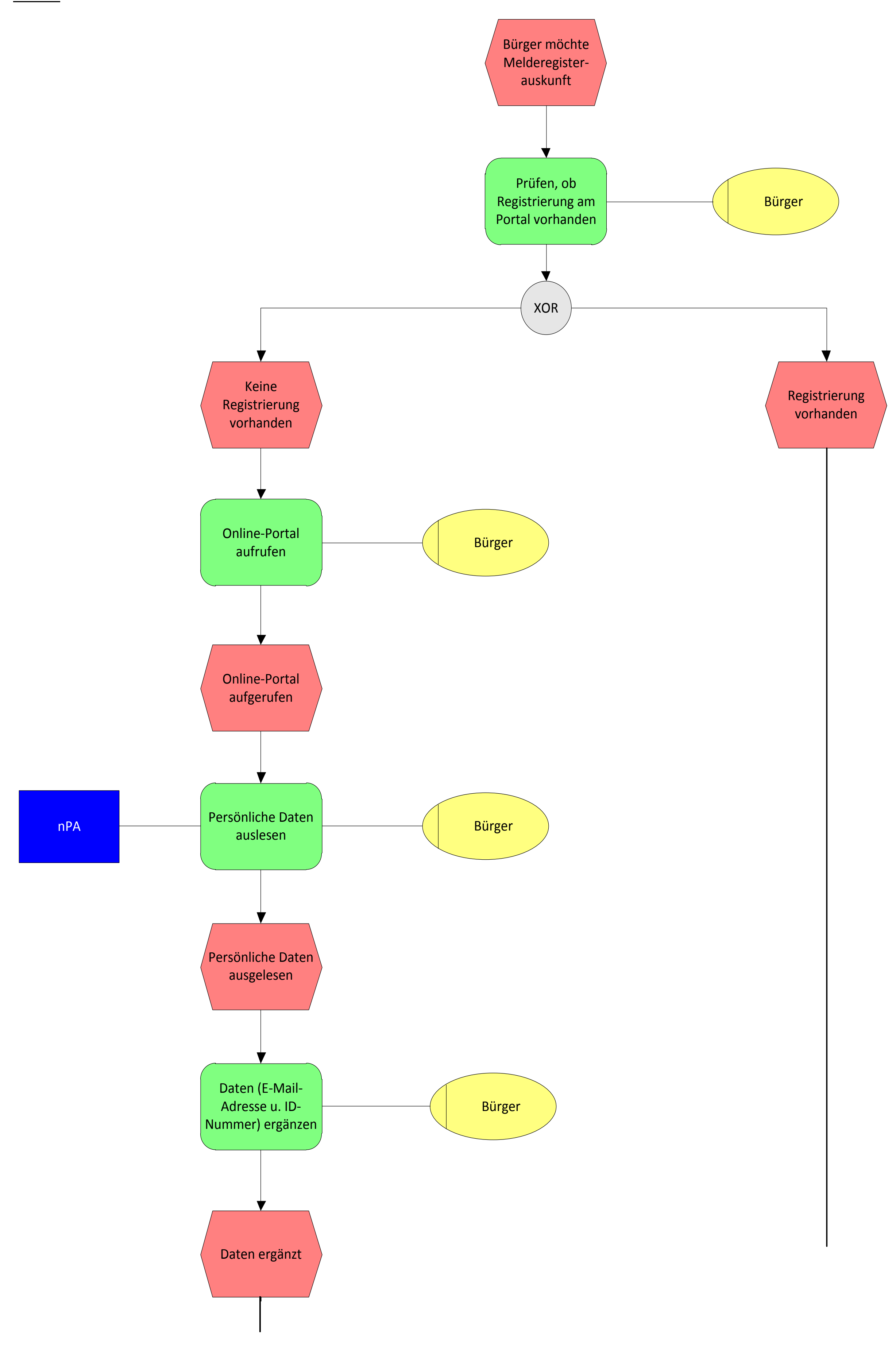
Gesamtauskunft mit nPA

Durch den neuen Personalausweis soll dieser Prozess vereinfacht und beschleunigt werden. Da die eID-Funktion des nPA die Feststellung der Benutzeridentität ermöglicht, kann sie die Anforderungen des MRRG erfüllen und bildet somit die Grundlage für eine Gesamtauskunft über ein Webportal.

Die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) hat im Rahmen des Pilotprojekts das Bürger-Service-Portal entwickelt. Dies ermöglicht den Bürgern die Gesamtauskunft online mithilfe des neuen Personalausweises einzuholen. Hierzu ist das Portal mandantenfähig, sodass es von jeder Behörde bzw. Gemeinde in den eigenen Webauftritt integriert werden kann, dadurch haben Bürger von jeder Webseite aus Zugriff, ohne sich um die genaue Zuständigkeit kümmern zu müssen. Das Portal nutzt die unter Anleitung des BSI entwickelte AusweisApp um die Authentifizierung durchzuführen und soll in Zukunft weitere Verwaltungsdienste bereitstellen (Mayer 2010, 8ff).

Nach dem Start der AusweisApp bekommt der Nutzer eine Übersicht, welche Daten von seinem Personalausweis an das System übermittelt werden bzw. zu übermitteln sind, um die Identität zweifelsfrei festzustellen. Der Bürger kann optional weitere Daten zur Übertragung freigeben. Nach Eingabe der sechsstelligen, persönlichen PIN, prüft der eID-Service Provider über die Public-Key-Infrastruktur die Identität des Nutzers und die Berechtigungszertifikate der Behörde. Ist dieser Schritt erfolgreich, liest die Behörde die freigegebenen Daten vom Ausweis und stellt den Gesamtbericht zusammen. Diesen Bericht kann der Bürger dann abrufen bzw. bekommt ihn auf der Weboberfläche des Bürger-Service-Portals angezeigt. Da die Rolle der Behörde nicht durch einen Mitarbeiter ausgefüllt werden muss, sondern durch ein automatisiertes System ersetzt werden kann, ist auf diesem Weg die Bescheinigung ohne längere Wartezeit für den Bürger sofort verfügbar. Eventuelle Gebühren können über das Bürger-Service-Portal auf verschiedene Arten eingezogen werden. (E-Payment, Lastschrift, Überweisung) (Mayer 2010, 10ff).

EPK:


Bürger möchte Melderegister-auskunft
Prüfen, ob Registrierung am Portal vorhanden
Bürger
XOR
Keine Registrierung vorhanden
Registrierung vorhanden
Online-Portal aufrufen
Bürger
Online-Portal aufgerufen
nPA
Persönliche Daten auslesen
Bürger
Persönliche Daten ausgelesen
Daten (E-Mail-Adresse u. ID-Nummer) ergänzen
Bürger
Daten ergänzt

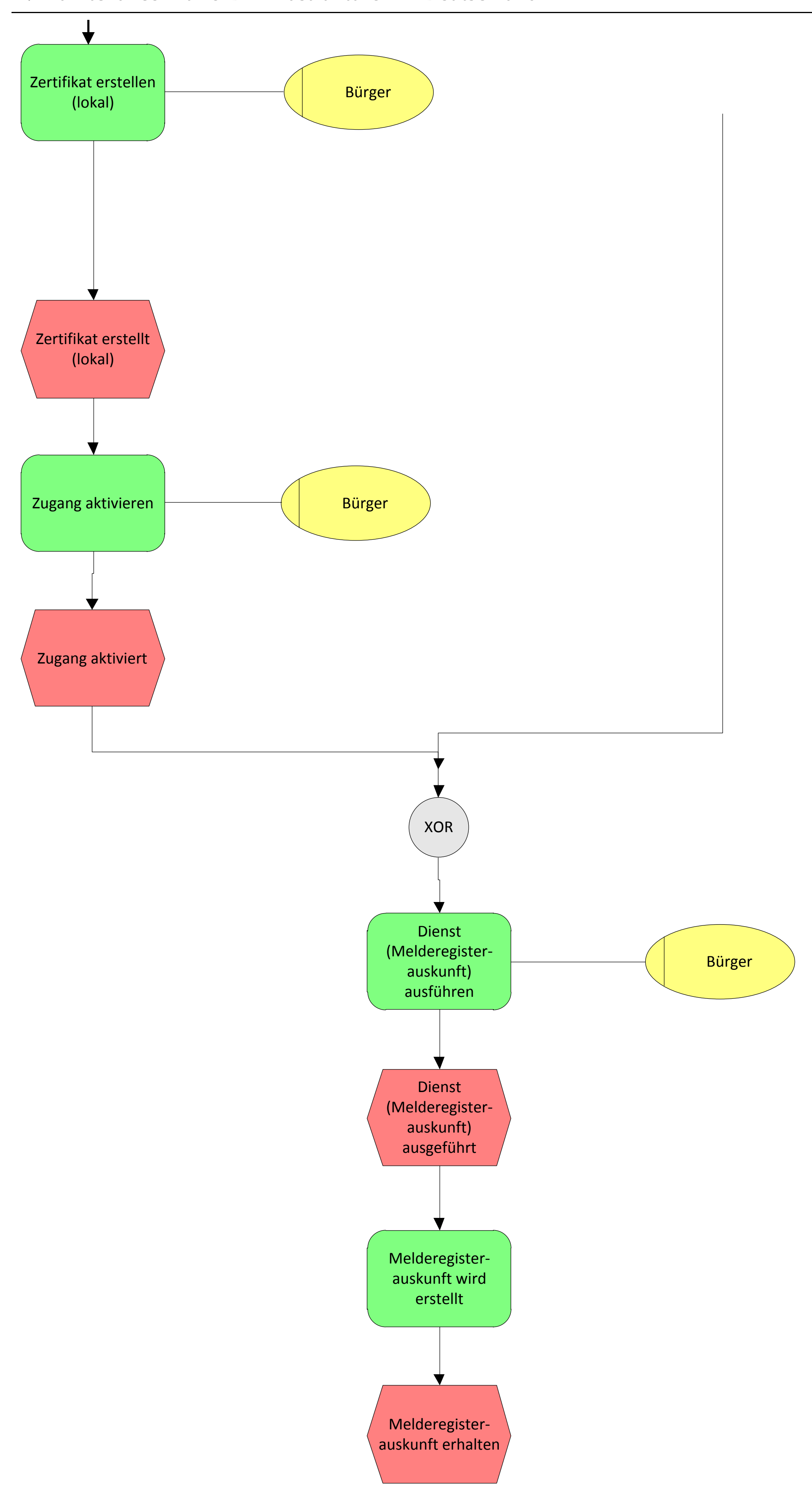


Abbildung 35: EPK Gesamtauskunft nach nPA-Einführung (Quelle: Eigene Darstellung)

Das Verfahren mit dem neuen Personalausweis hat einige Vorteile gegenüber dem jetzigen Stand. Es bietet für Bürger mehr Transparenz, da diese jederzeit eine Gesamtauskunft über die gespeicherten Daten einholen kann, ohne erst nach der für ihn zuständigen Behörde suchen zu müssen. Für die Behörde stellt es eine Erleichterung dar, da eine derartige Routineaufgabe verstärkt automatisiert abgewickelt werden kann.

Weitere Ergebnisse

Basierend auf den Experteninterviews können als Vorteile der nPA- bzw. AusweisApp-Einführung zunächst die Größe des nPA, die erstmalige Möglichkeit zur Online-Authentifizierung, die Möglichkeit zur medienbruchfreien Kommunikation, das elektronische Äquivalent zum Postident-Verfahren, eine flächendeckende, sichere Identifizierung im Internet oder in IT-Anwendungen, eine medienbruchfreie Verarbeitung von Anträgen gesehen werden. Aber durch den nPA wird es auch möglich, Prozesse, die bereits im Internet verfügbar sind, sicherer zu gestalten (wie z. B. Online-Banking). Außerdem können Prozesse, die heute noch nicht im Internet verfügbar sind, ins Internet gebracht werden. Das sind v. a. Prozesse, bei denen unbedingt eine Autorisierung erforderlich ist. Auf Seiten der Anbieter können außerdem organisatorische Vereinfachungen erreicht und dadurch Kosten gesenkt werden.

Als nachteilig werden v. a. Aspekte genannt, welche zusätzliche Kosten verursachen. Dies sind bspw. Kosten für den nPA, da dessen Kosten höher sind als die des konventionellen Personalausweises und für sichere Kartenlesegeräte, denn nur Lesegeräte der Klasse 3 sind sicher. Des Weiteren gibt es Bedenken hinsichtlich der AusweisApp: Bürger installieren sich die Software auf ihren Rechner, ohne zu wissen, ob bspw. bzgl. Bundestrojaner Gefahr davon ausgeht. Damit einhergeht, dass Bürger viel Verantwortung und Beweislast auf den Nutzer gelegt wird, was vorher nicht der Fall war. Derzeit liegt die Beweislast beim Anbieter. Weiter nachteilig für die Akzeptanz des nPA sind Sicherheitsbedenken und Misstrauen der Bürger gegenüber des nPA. Für Unternehmen entstehen durch den nPA zunächst erhebliche Investitionsaufwendungen, aber auch für Bürger entstehen Aufwendungen, zusätzlich müssen sich Bürger viel stärker mit dem Thema Sicherheit im Internet auseinandersetzen.

Als Hemmnisse hinsichtlich der AusweisApp werden v. a. technische, gesetzliche und gesellschaftliche Aspekte gesehen. Aspekte gesetzlicher Natur ist die bereits erwähnte Beweislast. Probleme gesellschaftlicher Natur werden darin gesehen, dass Anbieter auch mit technisch unerfahrenen Nutzergruppen zu tun bekommt. Auf der anderen Seite muss von den Nutzern ein sehr hohes technisches Verständnis aufgebracht werden, wodurch bestimmte Benutzergruppen ausgeschlossen werden. Ein weiterer gesellschaftlicher Aspekt ist, dass die Verfügbarkeit der gesamten zusätzlichen Onlinefunktionen nur da gegeben ist, wo Leute einen Onlinezugang haben (vgl. digitale Spaltung). Aber der Prozess hat auch Vorteile für Personen, die körperlich

eingeschränkt sind und deshalb nicht zur Behörde gehen können. Technische Hemmnisse bestehen hinsichtlich der digitalen Signatur, da die AusweisApp sich noch nicht einwandfrei in alle Anwendungen integrieren lässt. Des Weiteren fehlen derzeit noch Verschlüsselungszertifikate und die Benutzerführung ist wenig intuitiv, dadurch entstehen Schwierigkeiten für nicht technikaffine Personen. Als weitere Hindernisse hinsichtlich der AusweisApp werden auch mangelnde Organisation und der knappe Zeitplan für die Einführung angeführt.

Aus den Interviews konnte entnommen werden, dass vor allem Voraussetzungen technischer Natur, wie z. B. technische Richtlinien noch nicht ausgereift und zertifiziert sind und dies noch gelöst werden muss. Ein weiteres Problem, das es noch zu lösen gilt, ist der Umgang mit Berechtigungszertifikaten. Für jeden Dienst, den eine Kommune anbietet, wird ein Berechtigungszertifikat benötigt, was wiederum Kosten verursacht. Aus diesem Grund wird eine Anwendungsbündelung vorgeschlagen, d.h., ein Bündel von Diensten kann mit nur einem Berechtigungszertifikat abgewickelt werden. Dies würde ebenfalls eine finanzielle Entlastung der Behörden nach sich ziehen, da jedes Zertifikat Kosten im dreistelligen Bereich verursacht. Ein weiteres Problem, dass an dieser Stelle auftritt, ist die Abhängigkeit zwischen Ausweisinhaber und Diensteanbieter. Um den nPA für Bürger attraktiv zu machen, sollten eigentlich erst Anwendungen von den Diensteanbietern geschaffen werden, denn wenn Bürger sehen, dass viele Dienste für den nPA verfügbar sind, holen sie sich auch vor Ablauf der Frist einen neuen Personalausweis. Dies gilt vor allem für Personen, die einen neuen Ausweis beantragen wollen, obwohl der alte noch nicht abgelaufen ist. Auf der anderen Seite waren die Diensteanbieter ab, bis mehr Bürger einen nPA haben und bieten dann erst Dienste an. Ein weiteres Problem, das an dieser Stelle auftritt, ist die Hard- und Softwareverbreitung bei den Behörden.

Faktoren, die die nPA-Nutzung der Bürger beeinflussen, sind vor allem die Aussagen bzw. die Einstellung zum nPA des Verwaltungsmitarbeiters vor Ort im Bürgerbüro. Des Weiteren ist der Kostenfaktor ein wesentlicher Beeinflussungsfaktor: (sichere) Lesegeräte und Ausweis sollte billiger angeboten werden. Bürger werden ebenfalls von externen Faktoren beeinflusst. Durch die vielen Skandale, die den Datenschutz im Internet betreffen, sind Bürger grundsätzlich skeptischer geworden, was Nutzung und Versand eigener personenbezogener Daten im Internet angeht. Auch das Misstrauen hinsichtlich Sicherheit und Datenschutz gegenüber dem nPA beeinflussen Bürger. Positiv ist hingegen, die Erledigung des Behördengangs von zu Hause aus, also medienbruchfrei. Insgesamt muss gewährleistet werden, dass Bürger sich durch den nPA-Einsatz eindeutige Vorteile verschaffen, Sicherheitsgewinn für Bürger, obwohl dieser nicht mehr vor Ort sein muss, Eindeutige Feststellung der Identität der Bürger bspw. bei E-Commerce-Anwendungen, wodurch wiederum ein Sicherheitsgewinn für Bürger entsteht. Insgesamt muss die nPA-Nutzung für Bürger einfach, billig und attraktiv sein.

Maßnahmen, die die Nutzung hinsichtlich der Bürger steigern, sind eine einfache, gute und verständliche Benutzerführung sowie Informationen auf den jeweiligen Behördenhomepages und Hotlines. Nutzung kann auch durch die Einführung von Bürgerservice-Portalen gesteigert werden.

Aufgrund der in Kapitel 4.5.1 analysierten Szenarien können folgende Akzeptanzfaktoren nach Rogers zusammengefasst werden:

(1) *Relativer Vorteil:* Aus den Interviews kann entnommen werden, dass Vorteil für Bürger z. B. die eID-Funktion und die elektronische Signatur u.a. für E-Commerce-Anwendungen sind. Außerdem erhöht sich durch den nPA die Sicherheit, da nun im Internet ein eindeutiger Identitätsnachweis erbracht werden kann. Sind mehr Anwendungen im Internet verfügbar, können Bequemlichkeit, Flexibilität und Verfügbarkeit ebenfalls als Vorteile gesehen werden.

(2) *Kompatibilität:* Die Interviews ergaben, dass hinsichtlich der Kompatibilität des nPA in die bestehende Infrastruktur noch einige Herausforderungen zu bewältigen sind. Vor allem technisch-organisatorische Rahmenbedingungen bei den einzelnen Nutzern sind damit gemeint. Es sind neue Hardwarekomponenten nötig, die Lesegeräte, zudem benötigen die Nutzer (Bürger, Behörden, Unternehmen) einen internetfähigen Rechner und spezielle Software, die AusweisApp und Zertifikate.

(3) *Komplexität:* Aus den Szenarios des Anwendungstests ergab sich, dass z. B. eine verständliche Benutzerführung, welche durch grafische Elemente zur schnelleren Erlernbarkeit beitragen, wichtige Akzeptanzfaktoren sind. Des Weiteren erhöht die Bereitstellung von Supportfunktionen, wie Help Desk, Webseiten und Informationsmaterial die Akzeptanz der jeweiligen Dienste. Schaffung von Transparenz bspw. durch Implementierung von Sperremanagement und ein zentraler Ansprechpartner bei Diebstahl oder Verlust der PIN tragen zur Akzeptanz des nPA bei.

(4) *Erprobbarkeit:* Von Bürgern waren die analysierten Szenarios bislang noch nicht erprobbar, da dafür zunächst einmal der nPA benötigt wird. An den Anwendungstests nahmen nur vereinzelt Bürger teil und agierten als Kunden der beteiligten Wirtschaftsakteure. Der Anwendungstest unterstützt aber die Bewertung der Praxistauglichkeit, Handhabbarkeit, Akzeptanz und dient zur weiteren Entwicklung attraktiver Anwendungen.

(5) *Kommunizierbarkeit/Beobachtbarkeit:* Dieser Faktor wird erst dann möglich, wenn Bürger den nPA bereits haben, da nur aufgrund individueller Erfahrungen im Umgang mit und durch allgemeine Informiertheit über die Eigenschaften des nPA die Nutzer beobachten können.

5. Kommunikationsstrategien für eID-Projekte in Deutschland

Kommunikation spielt eine entscheidende Rolle bei der Einführung und Vermittlung von eGovernment-Infrastrukurprojekten, wie sie die eID darstellt. Die Erzeugung von Akzeptanz für neue Angebote der öffentlichen Hand ist eine eminent kommunikative Aufgabe (Morgan/Hunt 1994; Bart et al. 2005). Akzeptanz setzt insbesondere Vertrauen voraus, also die Bereitschaft, ein gewisses Risiko im Austausch mit Anderen einzugehen. Neue Angebote sind unweigerlich mit einem solchen, subjektiv wahrgenommenen Risiko verbunden.

Zahlreiche Forscher haben darauf hingewiesen, dass die Reputation eines Anbieters, also dessen zeitlich stabile Wahrnehmung und Einschätzung durch die Nutzer, einen starken Einfluss darauf hat, ob diese bereit sind, sich auf Transaktionen mit ihm einzulassen (Jarvenpaa et al. 2000; Walczuch/Lundgren 2004). Nutzer müssen also einem Anbieter neuer technologischer Lösungen vertrauen. Vertrauen kann dabei als ein Gefühl, eine Einstellung der Nutzer betrachtet werden - Kommunikation ist eine entscheidende treibende Kraft hinter der Entstehung und Pflege von Vertrauen (Grunig/Hunt 1984; Dozier/Ehling 1992). Die Beeinflussung dieser Wahrnehmungen, die Pflege der Reputation ist daher seit jeher die Aufgabe professioneller Kommunikation. Durch Kommunikation werden (potentielle) Nutzer mit Eindrücken und Informationen versorgt, welche der Beurteilung einer Vertrauenswürdigkeit zugrunde liegen.

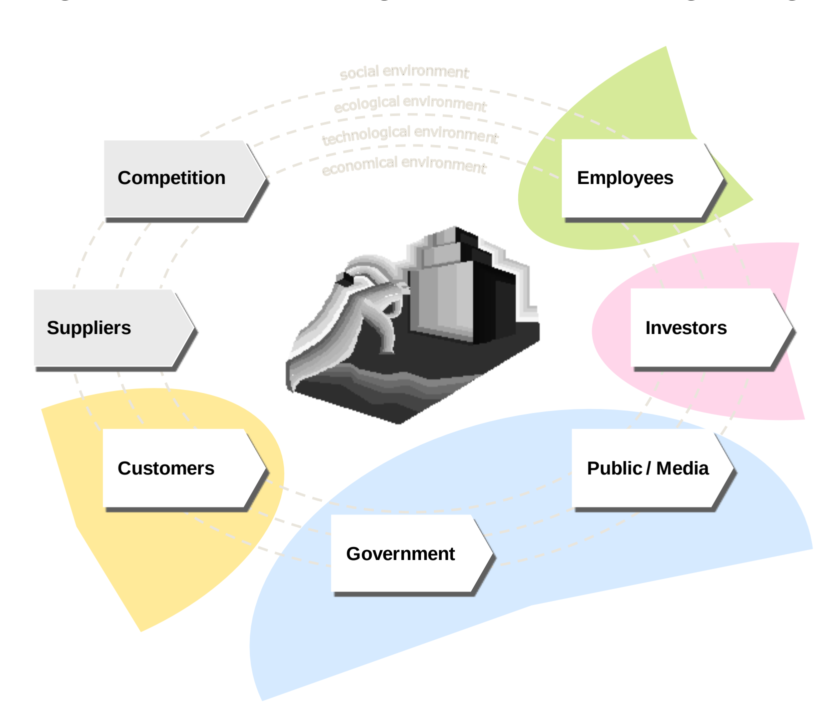


Abbildung 36: Anspruchsgruppen eines kommerziellen Angebots (Rüegg-Stürm 2003)

Jones et al. (2000) betonen dabei, dass die Etablierung von elektronischen Interaktionen keineswegs allein Nutzer und Anbieter einbinden, sie beruht vielmehr auf einem ganzen Netzwerk an Beziehungen mit zahlreichen diversen Anspruchsgruppen. Neben den Nutzern selbst sind

also auch die Mitarbeiter des Anbieters, dessen Kooperationspartner oder Intermediäre anzusprechen und in Kommunikationsbemühung einzubinden. Dies gilt auch und gerade für eGovernment oder eID Infrastrukturprojekte, die neben Bürgern auch Unternehmen und die Verwaltung sowie weitere Intermediäre einbinden. Kommunikationsstrategien haben daher den Aufbau und die Pflege vertrauensvoller Beziehungen zu bedeutenden Anspruchsgruppen und Kooperationspartnern zum Gegenstand. Sie umfassen die Einladung dieser Anspruchsgruppen zur Teilnahme an einer Transaktion, die Beschreibung der Identität und des Leistungsausweises eines Anbieters als vertrauenswürdiger Transaktionspartner, die Bereitstellung notwendiger Daten und Informationen für die Beurteilung der Vertrauenswürdigkeit, und die Sicherstellung der Zugänglichkeit und dialogischen Kommunikation, welche die Verlässlichkeit des Anbieters signalisiert und Vorbehalte abbaut (Shneiderman 2000).

(Chadwick 2001) stellt fest, dass Online-Transaktionen sich von physischen Transaktionen von Angesicht zu Angesicht vor allem darin unterscheiden, dass der Beziehungsaufbau durch technische Hürden erschwert ist. Nutzer interagieren mit Benutzeroberflächen, mit technischen Plattformen, nicht anderen Personen. Ein persönlicher Bezug fehlt in der Regel, auch werden elektronische Kontakte weniger in andere soziale Domänen übertragen. Elektronische Transaktionen stehen daher vor der Herausforderung, notwendige Informationen allein auf der Transaktionsplattform und im Rahmen der Transaktion bereitzustellen. Die Einbeziehung eines Kundendienstes kann hier zwar Abhilfe schaffen, führt jedoch unweigerlich zu einem Medienbruch.

Die Forschung betont entsprechend die Bedeutung der Transparenz und einer fairen sowie offenen Kommunikationspolitik für die Gewinnung von Nutzern für innovative Angebote. Demnach sollten Elemente wie Sicherheit, Schutz der Privatsphäre, Garantien und auch weitere Kundendienste proaktiv kommuniziert werden (Wang et al. 2004; Lanier/Saini 2008; Culnan/Armstrong 1999). Die so umschriebene Empfehlung ist jedoch durchaus nicht unumstritten. Einige Studien lassen Zweifel daran aufkommen, wie hoch die Aufmerksamkeit für Elemente wie Sicherheit und Privatheit im Rahmen einer realen Entscheidungssituation der Nutzer tatsächlich ist (Milne/Boza 1998).

Zweifellos erlauben technische Lösungen heute zahlreiche Ansätze und Möglichkeiten für Anbieter, ihre Nutzer anzusprechen und mit Informationen zu versorgen. Selbst virtuelle Kundendienste können eine Möglichkeit darstellen, persönliche Interaktionen zumindest zu simulieren (Urban et al. 2000). Nicht selten erlauben es neue Medien Nutzern auch, untereinander zu kommunizieren, und so Unterstützung und Entscheidungshilfen zu finden. Anbieter können online Applikationen für die Zustellung von Fragen, Anregungen oder auch Beschwerden installieren. Foren, Chats, Blogs oder auch Vlogs können Nutzer mit aktuellen Informationen versorgen und Kundendienste anbieten (Hart/Blackshaw 2005).

Kommunikationsstrategien im Rahmen von eID-Infrastrukturprojekten sind jedoch keine "one size fits all"-Lösungen. Unterschiedliche Anspruchsgruppen haben unterschiedliche Wünsche und Bedürfnisse wenn es um den Aufbau von Kooperationsbereitschaft und Akzeptanz geht (Shankar et al. 2002). Entsprechend ist es notwendig, unterschiedliche Kommunikationsstrategien zu identifizieren und differenzieren.

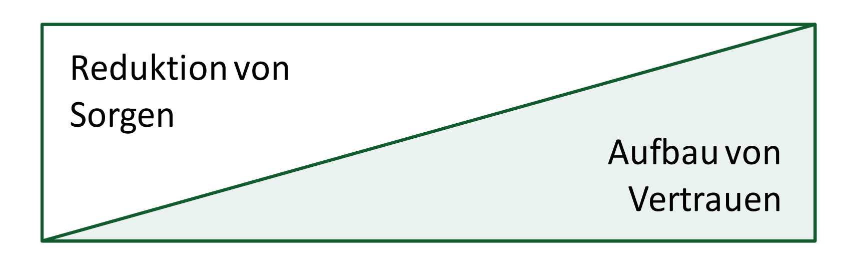


Abbildung 37: Unterschiedliche Schwerpunkte von Kommunikationsstrategien

Milne und Boza (1998) unterscheiden offensive von defensiven Kommunikationsstrategien: “In a concern-reduction strategy, communication is secretive, in an attempt to avoid consumers’ aversive responses. In this strategy, the optimal outcome is to avoid losing sales due to privacy concerns. In contrast, in a trust-building strategy, communication is informative and benefit driven, aimed at developing customer relationships.” Exzessive pro-aktive Kommunikation und eine möglichst umfangreiche Bereitstellung von Informationen zu Sicherheit und Privatheit einer Transaktion sind also nicht notwendigerweise optimale Strategien. Sie können im Gegenteil die Aufmerksamkeit auf kritische Aspekte einer Transaktion lenken und so Vorbehalte erst erzeugen. Alternativen bestehen darin, positive Bezüge zum Angebot herzustellen, dessen relative Vorteile oder Kompatibilität zu betonen. Kommunikationsstrategien haben aber in jedem Fall jene innovations- und personenbezogene Faktoren zu adressieren, die bereits als zentrale Treiber der Akzeptanz identifiziert wurden.

5.1. Vorgehen bei der Ermittlung der Kommunikationsstrategien

Die Identifikation von Kommunikationsstrategien im Rahmen der Einführung von eID Anwendungen erfolgte parallel zur oben beschriebenen Analyse der Marktmodelle und -chancen. Es wurden daher ebenfalls die erwähnten Anwendungsszenarien zugrunde gelegt (vgl. Abbildung 23):

(1) Kfz-Zulassung
(2) ELSTER
(3) Emissionshandel
(4) Gewerbeanmeldung
(5) Gesamtauskunft

Hier wurden qualitative Experteninterviews mit je ein bis zwei Vertretern der Teilnehmer an den Anwendungsszenarien durchgeführt, transkribiert und ausgewertet. Alle Interviews folgten einem einheitlichen Leitfaden. Dieser basierte auf den in Kapitel 2 definierten Einflussfaktoren der Nutzerakzeptanz (innovationsbezogene ebenso wie nutzerbezogene Faktoren). Angesprochen wurden Eigenschaften der angebotenen Innovation, wie relative Vorteile und Nutzen, Komplexität, Applikationshürden und Kompatibilität, Dispositionsfaktoren wie spezifische Eigenschaften einer abgrenzbaren Zielgruppe sowie die gewählten Kommunikationsmassnahmen, -instrumente, Vertriebskanäle und Kundendienstangebote. Ziel der Befragung war es also, Kommunikationsstrategien zu charakterisieren und differenzieren, basierend auf ihrer Berücksichtigung wesentlicher Treiber der Nutzerakzeptanz.

5.2. Kommunikationsstrategien der Anwendungsszenarien

Im Folgenden werden die Kommunikationsstrategien der beteiligten Partner im Rahmen der verschiedenen Anwendungsszenarien differenziert beschrieben.

5.2.1. Kfz-Zulassung

Dispositionsfaktoren

Derzeit richtet sich das Angebot an eine sehr begrenzte Zielgruppe: Autokäufer in Berlin (Neuanmeldungen), welche über den nPA verfügen. Im Rahmen des Pilotprojekts beschränkt sich die Kooperation darüber hinaus auf ein spezifisches Autohaus sowie einen Anmeldungsdienstleister. Damit ist der Adressatenkreis weiter eingeschränkt, jedoch bestehen mit Ausnahme der Volljährigkeit und gewissen materiellen Voraussetzungen keine systematischen Beschränkungen der Zielpersonen. Geplant wäre mittelfristig eine Ausweitung des Angebots auf alle Zulassungsstellen und Autohäuser sowie verschiedene Dienstleister. Aussagen über eine systematische Bevorzugung des Angebots durch spezifische soziodemographische Segmente der Bevölkerung können zum Erhebungszeitpunkt jedoch nicht getroffen werden.

Innovationsgrad

Der relative Nutzen des Angebots wird vor allem in einer Prozess**beschleunigung** gesehen, welche neben dem Nutzer auch den Intermediären sowie der Verwaltung zu Gute käme. Darüber hinaus wird eine **Transparenz**steigerung des Prozesses erzielt, indem Statusmeldungen unterschiedlicher Bearbeitungsstufen generiert werden. Dadurch wird auch möglichen Brüchen im Prozess aufgrund mangelhafter Integration unterschiedlicher notwendiger Prozesseschritte entgegengewirkt. Die **Bequemlichkeit** und **Sicherheit** des Prozesses soll ebenfalls erhöht werden, da die elektronische Anmeldung keine physische Abgabe der ID mehr erforderlich macht. Ausweisverluste werden so ausgeschlossen. Hinzu

kommen andererseits mögliche Gefährdungen durch denkbare Beeinträchtigungen der elektronischen Übermittlung.

Der Innovationsgrad ist aus Sicht der Endnutzer überschaubar, da es sich vor allem um eine Adaption eines bestehenden Prozesses handelt - und damit eine Beschleunigung. Der Anwendungskontext ist bekannt und bleibt unverändert (hohe Kompatibilität). Aufgrund der Betreuung der Nutzer im Rahmen der Nutzungssituation durch Vertreter des Autohauses und des Dienstleisters ist eine Überforderung durch das Angebot unwahrscheinlich (geringe Komplexität).

Applikationshürden

Im Rahmen des Pilotprojekts erfolgt die Bedienung des neuen Angebots weitgehend durch Repräsentanten des Autohauses sowie Vertreter des Dienstleisters. Diese werden entsprechend in der Anwendung der neuen Prozesse geschult. Ein spezifisches Nutzer-**Know How** ist daher nicht erforderlich. Auch bestehen aus Nutzer-Sicht keine **materiellen Hürden**, da die Infrastruktur, wie bspw. Lesegeräte, vor Ort angeboten wird. Dies könnte sich jedoch ändern, sofern eine flächendeckende Ausweitung des Angebots erfolgt.

Vermittlung

Die Vermittlung des Pilotprojekts erfolgt nahezu ausschliesslich über den Vertriebskanal Autohaus. Dort stehen **Repräsentanten** bereit, welche notwendige Schritte und Abläufe beschreiben, Vorteile erklären und Fragen beantworten können. Auch ein Kundendienst ist somit vor Ort gegeben. Informationen zum Angebot werden so aggregiert und aufgearbeitet, dass sie am "**Point of Sale**" vermittelt werden können. Entsprechend wird davon ausgegangen, dass das Autohaus das neue Angebot bewerben wird, wobei spezifische Werbemassnahmen zum Erhebungszeitraum nicht bekannt waren. Ebenso waren von Seiten des involvierten Dienstleisters Massnahmen der Öffentlichkeits- und Pressearbeit geplant, sowie eine Vorstellung des Angebots im Rahmen von Messe-Präsenzen. Mittelfristig ist hier auch eine Bewerbung elektronischer Angebote über Online-Medien (u.a. SEO-Marketing) angedacht.

5.2.2. ELSTER

Dispositionsfaktoren

Das Angebot richtet sich an eine breite Zielgruppe: alle steuerpflichtigen Bürger können auf die Elektronische Steuererklärung zugreifen. Es ist bisher nicht bekannt, ob es bei der tatsächlichen Nutzung des Angebots zu systematischen Differenzierungen der Nutzergruppen kommt, angesichts der breiten Akzeptanz des Angebots wird dies jedoch nicht vermutet.

Neben den steuerpflichtigen Bürgern wurden auch die Beamten der Steuerverwaltung als Zielgruppe des ELSTER-Projekts definiert.

Innovationsgrad

Der relative Vorteil des Angebots wird vor allem in einer **Beschleunigung** und **Vereinfachung** eines etablierten Prozesses gesehen. Ein Medienbruch wird vermieden, die direkte Datenübermittlung erleichtert die elektronische Datenverwaltung.

Die Einbindung der eID verändert den Prozess der ELSTER nicht grundlegend, sie führt lediglich zu einer weiteren Vereinfachung. Mit der Übertragung der Identifikation auf die elektronische Kommunikation werden auch hier Medienbrüche vermieden, Unsicherheiten durch postalische Übermittlungen werden reduziert, gleichzeitig steigen jedoch die Anforderungen an die Sicherheit der elektronischen Datenverarbeitung.

Aus Sicht der Nutzer liegt ein erhöhter Innovationsgrad in der Nutzung der elektronischen Steuererklärung. Ist dessen Bedienung erlernt, so stellt die Einbindung der eID Funktion lediglich eine Erweiterung dieses innovativen Verfahrens dar. Auf Basis des ELSTER-Angebots ist die eID-Nutzung somit von hoher Kompatibilität, sie weist jedoch eine gewisse zusätzliche Komplexität auf.

Applikationshürden

Eine Applikationshürde besteht zweifellos in der Umstellung der Steuererklärung auf ein elektronisches Verfahren. Angesichts der nicht unbeachtlichen Komplexität des zugrundeliegenden Prozesses (Steuererklärung) stellt dessen Transfer auf ein elektronisches Angebot jedoch - die notwendigen Fähigkeiten zur Bedienung vorausgesetzt - tatsächlich an vielen Stellen eine Vereinfachung dar. Mit diesem Umstand ist vermutlich die bereits hohe Akzeptanz des Angebots zu erklären. Hinzu kommt, dass gewisse Aspekte der Nutzung obligatorisch sind.

Durch die ELSTER-Nutzung entstehen in einem ersten Schritt **keine Einstiegskosten**. Der Zugang ist durch den Web-Browser oder bestehende Software-Angebote möglich. Die Integration der eID Funktion ist mit den üblichen Aufwänden für die private nPA-Nutzung verbunden (Ausweis, Lesegerät). Auch ist der Umgang mit dem nPA entsprechend zu erlernen. Insgesamt legt das ELSTER-Projekt hohen Wert auf ein nutzerfreundliches Design des Angebots sowie auf eine **einfache Bedienbarkeit**, insbesondere um damit auch die Vorzüge des elektronischen Angebots vermitteln zu können.

Vermittlung

Nachdem die Bundesländer für den Steuervollzug zuständig sind, ist auch die Kommunikation oder Bewerbung des ELSTER-Angebots Ländersache. Die Träger des ELSTER Projekts haben jedoch eine AG Marketing eingerichtet, welche Materialien erarbeitet, die bundeseinheitlich Anwendung in der Kommunikation finden können. Die Verantwortung für die AG liegt federführend beim Bundesland Niedersachsen, die Betreibung des Portals liegt in der Verantwortung des Freistaats Bayern.

Die AG Marketing legt grossen Wert auf einen einheitlichen Aussenauftritt des Projekts. So wurde "ELSTER" als **Marke** des Projekts festgelegt, ein **Logo** für das Angebot erarbeitet, ebenso wie ein einheitliches **Corporate Design**. Der AG steht ein Budget für die Erstellung von Informationsmaterialien zur Verfügung. Hierzu zählen **Messeauftritte, Plakate, Flyer**, auch Briefe an die Zielgruppen. Die Nutzung dieser Instrumente liegt in der Verantwortung der Bundesländer. Die Instrumente können hier etwa mit dem Landeswappen versehen werden, die Produktionskosten liegen entsprechend auch bei den Ländern.

Als führendes Mitglied des Projekts kommuniziert das Bundesland Bayern das Angebot sehr offensiv. Neben den beschriebenen Materialien setzte der Freistaat etwa auch ein Gewinnspiel ein, um Nutzer für das Angebot zu gewinnen. Dieses **Gewinnspiel** wurde wiederum mit eigens erstellten Materialien, wie etwa Plakaten, beworben. Das Corporate Design ebenso wie der gemeinsame Webauftritt stellen dabei jedoch die bundesweite Einheitlichkeit des Auftritts gegenüber den Nutzern sichern.

Die Vermittlung des Angebots wendet sich nicht alleine an die Bürger, die Mitarbeiter der Ämter wurden ebenfalls als eine wichtige Zielgruppe erkannt. Die AG verbreitet daher Schreiben an die Beamten und führt "**ELSTER Tage**" für ihre Schulung durch. In den Ämtern soll so jeweils ein ELSTER Botschafter definiert werden, die Ämter sollen aktiv dazu beitragen, dass die Nutzung durch die Bürger erhöht wird. Neben ihren Ansprechpartnern in den Finanzämtern steht den Bürgern nicht zuletzt auch ein Kundendienst zur Verfügung. Die entsprechende Hotline wird durch einen externen Dienstleister betrieben.



Abbildung 38: Website des ELSTER-Angebots

5.2.3. Gewerbeanmeldung

Dispositionsfaktoren

Das Angebot richtet sich an eine spezifische Zielgruppe, jene der Unternehmensgründer. Jährlich werden in Deutschland etwa 800.000 Unternehmen angemeldet, darunter überwiegend Klein- und Nebenerwerbsbetriebe. Die anmeldenden Personen sind in etwa 70% der Fälle männlich, jedoch aus unterschiedlichen Altersgruppen und Haushaltszusammensetzungen. Soziodemographisch handelt es sich somit um eine durchaus breit gestreute Zielgruppe. Betrachtet wurde im konkreten Falle die elektronische Gewerbeanmeldung im Bundesland Baden-Württemberg.

Innovationsgrad

Die elektronische Gewerbeanmeldung stellt erneut vor allem eine Übertragung vorhandener Prozesse auf eine elektronische Infrastruktur dar. Die Prozesskomplexität wird dadurch tendenziell reduziert, Medienbrüche werden vermieden. Als Vorteile werden somit vor allem eine **Vereinfachung** und auch mögliche **Beschleunigung** des Verfahrens gesehen. Das bisherige Angebot einer elektronischen Gewerbeanmeldung war nur auf geringe Verbreitung getroffen, weil der Prozess eine elektronische Signatur erforderte, die jedoch nur wenig verbreitet ist.

Die eID-Funktion des nPA stellt eine wichtige Möglichkeit der Identifikation im Prozess dar, eine signifikant höhere Akzeptanz des Verfahrens wird jedoch erst erwartet, wenn hierfür eine elektronische Signatur nicht mehr erforderlich ist. Das Erfordernis einer elektronischen Signatur erhöht die Komplexität des Angebots, reduziert die Kompatibilität und steigert somit auch die Applikationshürden.

Auch mit Ausnahme der Signatur ist die Kompatibilität des Angebots einer elektronische Gewerbeanmeldung nicht als sehr hoch einzuschätzen, da die Betriebsgründung in der Regel mit Behördengängen über die reine Anmeldung hinaus verbunden ist. Sofern also ohnehin ein persönlicher Kontakt und Austausch mit dem zuständigen Amt besteht, ist die elektronische Abwicklung nur eines Elements des Verfahrens als keine signifikante Vereinfachung zu betrachten.

Applikationshürden

Bei der Gestaltung der elektronischen Gewerbeanmeldung wurde stark auf die **Nutzerfreundlichkeit** des Angebots geachtet. Ein Assistent vereinfacht hier das Ausfüllen der Formulare. Auf dieser Seite werden daher keine Applikationshürden gesehen. Das Anmeldeverfahren verfügt über eine gewisse Komplexität, die jedoch durch seine elektronische Abwicklung tendenziell reduziert wird.

Nutzungshürden werden vor allem in der notwendigen Identifikation ausgemacht. Neben der notwendigen Infrastruktur für die eID Funktionalität des nPA ist hierzu vor allem die **elektronische Signatur** und die mit der Nutzung verbundenen Kosten zu zählen.

Vermittlung

Die elektronische Gewerbeanmeldung wird vor allem über die Webauftritte der Kommunen vermittelt. Das Angebot soll in deren Websites, bzw. "**virtuelle Rathäuser**" integriert werden. Die Information zum Angebot oder dessen aktive Bewerbung würde entsprechend auch in der Verantwortung der Kommunen liegen. Hier sind bisher keine nennenswerten Aktivitäten bekannt.

Neben den kommunalen Webseiten wird das Angebot auch über eine landesweite Plattform vertrieben, das "Service BW"-Portal. Der Kundendienst, etwa im Falle von Rückfragen oder Bedienschwierigkeiten, wird jedoch erneut durch die zuständigen **Gewerbeämter** auf kommunaler Ebene angeboten. Darüber hinaus besteht auch die Möglichkeit zur Inanspruchnahme der bundeseinheitlichen Behördennummer 115.

5.2.4. Emissionshandel

Dispositionsfaktoren

Das Angebot des elektronischen Emissionszertifikatehandels konzentriert sich auf betriebliche Nutzer, es handelt sich also um ein B-2-G-Angebot. Unter den betrieblichen Nutzern verfügt das Angebot aber über eine breite Nutzerbasis, da neben den inländischen auch ausländische Nutzer mit dem Anbieter interagieren. (Dabei richtet sich die Einbindung einer eID-Funktionalität auf Basis des nPA offensichtlich ausschliesslich an die inländischen Nutzer.) Nachdem die Nutzung des Angebots in der Regel in einem betrieblichen Kontext stattfindet und die Nutzung obligatorisch ist, ist nicht mit einem signifikanten Einfluss von Dispositionsfaktoren zu rechnen.

Innovationsgrad

Eine elektronische Anmeldung bei der DEHSt ist schon heute möglich und wird rege genutzt. Die Einbindung der eID Funktionalität in diesen Prozess soll vor allem die **Sicherheit** des Angebots erhöhen. Hieran äussern insbesondere die Nutzer gegenüber dem Anbieter ein hohes Interesse, da zum Teil sensible Daten und Informationen mit den Anmelde- und Nutzungsverfahren verbunden sind. Die Medienbruchfreiheit reduziert die Wahrscheinlichkeit von Eingabefehlern seitens des Kontobevollmächtigten. Die elektronische Datenverarbeitung kann darüber hinaus gegenüber dem Versandweg Sicherheitsvorteile aufweisen.

Die Komplexität der Einbindung einer eID Funktionalität in den Anmeldeprozess wird als gering betrachtet, die Kompatibilität ist dagegen hoch, da der **Anwendungskontext bekannt** ist und der Prozess im Austausch mit dem Nutzer eher vereinfacht und beschleunigt wird.

Applikationshürden

Während die Nutzung des Angebots obligatorisch ist, ist die Nutzung des elektronischen Verfahrens freiwillig. Die bekannten **Kosten** der nPA-Nutzung sind im Rahmen einer betrieblichen Anwendung wohl als zu vernachlässigen zu betrachten. Die Nutzung des Angebots erfordert bereits heute eine gewisse Reflexionstiefe und ist mit hohen **Sicherheitsanforderungen** verbunden. Die Umstellungs- oder Einstiegshürden sind daher nicht als hoch zu bewerten. Im Gegenteil wird von Seiten des Anbieters eher die mangelnde Verbreitung und Verfügbarkeit des nPA als mögliches Nutzungshemmnis betrachtet.

Ein zentrales Anliegen im spezifischen Anwendungskontext ist die Sicherheit des Verfahrens. Sofern der Anbieter glaubwürdig kommunizieren kann, dass das neue Angebot mit einer erhöhten Sicherheit verbunden ist, sollten weitere Vermittlungshürden in den Hintergrund treten. Andererseits ist insbesondere in dieser Glaubwürdigmachung eine Herausforderung der Angebotsvermittlung zu sehen. Andere Elemente, wie etwa die Nutzerfreundlichkeit, treten dagegen in ihrer relativen Bedeutung zurück.

Vermittlung

Die Vermittlung des Angebots erfolgt in der Kundenkommunikation der DEHSt mit den heutigen und künftigen Nutzern. Diese wurden bereits über die geplante Implementierung der eID Funktionalität informiert. Sobald die Implementation der entsprechenden Prozesse abgeschlossen ist, soll die Verfügbarkeit des Angebots ebenso mitgeteilt werden. Dabei soll die Nutzung des neuen Angebots insbesondere aufgrund ihrer Vorteile in Hinblick auf die Prozesssicherheit empfohlen werden.

Die verfügbaren Kanäle der Kundenkommunikation beschränken sich vor allem auf die **Website** des Anbieters, das verfügbare **Nutzerhandbuch** sowie gelegentliche **Rundschreiben**. Die Informationen zum neuen Angebot sollen hier in die etablierten Kommunikationsprozesse einfliessen. Weitergehende Massnahmen oder Instrumente darüber hinaus sind nicht geplant.

Bisher wurde die Erfahrung gemacht, dass von Seiten der Medien ein gewisses Interesse an der Einbindung und den Vorteilen des neuen eID-Angebots besteht. Vor diesem Hintergrund ist geplant, nach Abschluss der Implementation auch die Pressearbeit der DEHSt in den Vermittlungsprozess einzubinden. Angestrebt würde eine gewisse Aufmerksamkeit insbesondere in der relevanten **Fachpresse**, um auch so bestehende und künftige Kunden zu erreichen.

Ein **Kundendienst** wird bereits heute in Form einer Hotline angeboten, welche durch ein entsprechendes Referat betreut wird. Auch im Rahmen der Einführung des neuen Angebots wird dieser Kundendienst als Anlaufstelle für Fragen und Hilfestellungen dienen. Weitergehende Fachfragen werden intern an die entsprechend verantwortlichen Stellen weitergeleitet werden.

5.2.5. Gesamtauskunft

Dispositionsfaktoren

Das Angebot der Gesamtauskunft richtet sich als verpflichtendes Angebot der Behörden an alle betroffenen Bürger, und damit an eine sehr breite Zielgruppe. Die Anbieter gehen jedoch davon aus, dass tendenziell vor allem jüngere und technikaffine Bürger tatsächlich Gebrauch von einer elektronischen Gesamtauskunft machen würden. Da die Einführung des Angebots in einer ersten Pilotphase in Kooperation mit wenigen ausgewählten bayerischen Kommunen geschehen wird, schränkt sich die effektive Zielgruppe vorerst auf deren Bewohner ein.

Neben den Bürgern sind auch die Kommunen als Zielgruppen des Angebots zu bezeichnen. Absicht des Anbieters AKDB ist es, Kommunen von den Vorteilen und letztlich der Nutzung des Angebots zu überzeugen. Die Weitervermittlung des Angebots an die Bürger erfolgt anschliessend durch die teilnehmenden Kommunen.

Innovationsgrad

Erneut handelt es sich beim beschriebenen Angebot um die elektronische Abwicklung eines bekannten und etablierten Prozesses. Aus Sicht des Bürgers ist ein Vorteil vor allem mit der **Bequemlichkeit** verbunden, den Prozess von einem beliebigen Rechner aus durchführen, einen Behördengang also vermeiden zu können. Damit kann auch ein **Zeitgewinn** verbunden sein. Erforderlich für eine Nutzung der elektronischen Gesamtauskunft ist vor allem die Fähigkeit zum Umgang mit der entsprechenden Benutzeroberfläche, sowie der notwendigen IT Infrastruktur. Es hängt somit von den Fähigkeiten und Erfahrungen des Nutzers ab, wie die Komplexität des Angebots, vor allem relativ zum bisherigen, einzuschätzen ist.

Auf Seiten der anbietenden Behörden wird vor allem ein Vorteil in der Kosteneffizienz des Angebots gesehen. Sofern die Gesamtauskunft durch den Bürger selbständig und elektronisch durchgeführt wird, ist auf Behördenseite sowohl eine Ressourceneinsparung bei den Fix- wie auch den variablen Kosten denkbar. In jedem Fall könnte sich aus dem elektronischen Angebot eine Arbeitsentlastung ergeben.

Applikationshürden

Sofern ein Bürger sein Recht auf eine umfassende Datenauskunft in Anspruch nehmen möchte, stehen ihm der Gang zu seiner zuständigen lokalen Behörde oder im Falle der Pilotkommunen künftig der

direkte elektronische Abruf der Daten zur Verfügung. In beiden Fällen ist der Vorgang mit einem überschaubaren Aufwand für den Bürger verbunden. Im Falle der elektronischen Auskunft erfordert der Prozess die Bedienung der **Nutzeroberfläche**, während andernfalls eine persönliche Beratung auf dem Amt zur Verfügung stünde. **Umstellungskosten** sind lediglich die üblichen mit dem nPA verbundenen (Ausweis, Lesegerät).

Vermittlung

Das Angebot der elektronischen Gesamtauskunft erfolgt letztlich über die lokalen Behörden. Der Anbieter AKDB stellt die Infrastruktur, darunter auch die Nutzeroberfläche des Angebots. Diese wird in die **Websites** der am Pilotprojekt teilnehmenden Kommunen eingebunden. Aus Sicht der Bürger besteht hierin also der primäre Kommunikationskanal.

Die Kommunikation des Anbieters AKDB konzentriert sich vor allem auf die Zielgruppe der Kommunen - diese sollen von einer Nutzung des Dienstes überzeugt werden. Die darüber hinausgehende Ansprache der Bürger ist den **Kommunen** überlassen. Zum Erhebungszeitraum war nicht bekannt, dass diese weitergehende Werbemassnahmen planen, um auf das neue Angebot aufmerksam zu machen.

Der **Kundendienst** erfolgt wie bei der bisherigen Gesamtauskunft auch letztlich über die zuständigen kommunalen Behörden. Fragen technischer Natur der Behörden werden durch den Anbieter bearbeitet.

5.2.6. Zusammenfassung

Die fünf untersuchten Anwendungsszenarien stellen tatsächlich sehr unterschiedliche e-Government Angebote auf Basis der eID Funktion des nPA dar. Differenzen lassen sich unter anderem in den folgenden Bereichen feststellen:

Zielgruppe

Die Angebote richten sich zum Teil an breite Bevölkerungsschichten und sind jedem volljährigen Bürger zugänglich, sofern die geographische Verbreitung gegeben ist (Gesamtauskunft, ELSTER). Andere Angebote sind nur im Kontext spezifischer Geschäftsvorfälle von Belang und richten sich daher an ein kleineres Segment der Bevölkerung, ohne jedoch tatsächlich andere auszuschliessen (Kfz-Zulassung, Gewerbeanmeldung). Schliesslich wurde auch ein Angebot betrachtet, dass vorwiegend im Austausch zwischen betrieblichen Nutzern und der Verwaltung Anwendung findet (Emissionshandel).

Demographische Ausschlusskriterien sind mit Ausnahme eines Mindestalters keine vorhanden. Auch werden in der Regel keine formellen Zugangshürden errichtet (Bildung, Erfahrung, etc.), eine Fähigkeit zur Nutzung einer IT Infrastruktur wird jedoch bis auf einen Fall (Kfz-Zulassung) in aller Regel vorausgesetzt. Vereinzelt wird darüber spekuliert, dass das Angebot bei gewissen Nutzergruppen bevorzugt Anwendung finden könnte (etwa jüngere, technikaffine Nutzer). Diesbezügliche Erfahrungs-

werte liegen jedoch nicht vor. Auch werden in keinem Fall die Kommunikationsstrategien gezielt auf solche Gruppen zugespitzt.

Anwendungskontext

Eng mit den Zielgruppen verbunden ist die Bandbreite der Anwendungskontexte, so werden die Angebote zum Teil im privaten Kontext genutzt (Gesamtauskunft), zum Teil im geschäftlichen (Emissionshandel). Manche Angebote sind für beide Kontexte relevant (ELSTER, Kfz-Zulassung). In der Regel sind die Angebote zum Zeitpunkt der Erhebung freiwillig, oder zumindest nur zu Teilen obligatorisch. Nachdem keines der Angebote jedoch spezifisch auf einen Freizeit-Kontext ausgerichtet ist, ist in jedem Fall bevorzugt von einer sachlichen, transaktionsbezogenen Tonalität und Botschaft in der Kommunikation auszugehen.

Weitergehende mögliche Kontextfaktoren, wie etwa kulturelle, politische, mediale oder infrastrukturelle Einflussfaktoren wurden im Rahmen der Erhebung nicht weitergehend analysiert, können aber einen Einfluss auf die Wahl einer angemessenen Kommunikationsstrategie entfalten.

Innovationsgrad

In allen betrachteten Fällen handelt es sich bei den Angeboten um die Übertragung eines bestehenden und bekannten Prozesses auf die elektronische Kommunikation, so dass den Nutzern künftig neben dem physischen Austausch die Möglichkeit eines elektronischen zur Verfügung steht. In manchen Fällen bestand auch schon zuvor die Möglichkeit eines elektronischen Austausches, dieses Angebot wird durch die Einbindung der eID lediglich verbessert oder erweitert (Emissionshandel, ELSTER). Sofern die elektronischen Angebote sich in Ablauf oder auch Erscheinung an den bestehenden physischen orientieren, ist von einem begrenzten Innovationsgrad auszugehen - die Nutzer haben sich nicht an völlig neue Dienste oder Prozesse zu gewöhnen. Damit ist die Komplexität der Angebote in der Regel eher gering, die Kompatibilität relativ hoch. Auch werden die Prozesse nicht grundlegend verändert, in aller Regel wird vor allem darauf abgezielt, sie schneller, bequemer, sicherer und gegebenenfalls kostengünstiger zu gestalten. Dies sind entsprechend die relativen Vorteile, die in der Kommunikation berücksichtigt werden.

Applikationshürden

Wesentliche Umstellungskosten sind in der Regel nicht mit den neuen Angeboten, sondern vielmehr mit der Einbindung der eID verbunden. Die einzig relevanten zusätzlichen Nutzungskosten gehen mit der Nutzung des nPA einher (Lesegerät, Ausweis, Signatur). Eine Vermittlungshürde kann ebenfalls im Umgang mit dem nPA sowie dessen Infrastruktur gesehen werden. Sofern die Bürger sich jedoch an dessen Einsatz zur elektronischen Identifikation gewöhnt haben, bestehen kaum Anwendungshürden der darauf basierenden Angebote.

Die Anbieter legen in der Regel Wert auf die Nutzerfreundlichkeit in der Gestaltung des Angebots, so dass die elektronischen Dienste teilweise als nutzerfreundlicher betrachtet werden, als die physischen Alternativen (Gewerbeanmeldung, ELSTER). Dabei ist zu berücksichtigen, dass die Nutzerfreundlichkeit des Designs je nach Anwendungskontext unterschiedliche Bedeutung hat - sie steigt, sofern es sich um ein freiwilliges Angebot für die private Nutzung durch eine breite Masse der Bürger handelt, und sinkt entsprechend im Falle obligatorischer, geschäftlicher und sehr spezifischer Anwendungsfälle.

Die Ein- oder Umstiegshürden werden über alle Fälle hinweg als tief betrachtet, da - sofern eine IT Infrastruktur und eine gewisse grundlegende Befähigung zum Umgang mit dieser vorhanden sind - kaum zusätzliche Fertigkeiten vorausgesetzt werden. Dies gilt insbesondere, da es sich in der Regel um bekannte oder etablierte Angebote und Prozesse handelt, die lediglich auf die elektronische Kommunikation übertragen werden.

Auf Unterschiede in den Vermittlungsansätzen soll im folgenden Abschnitt eingegangen werden.

5.3. Generalisierung der Kommunikationsstrategien

Eine Analyse der Gemeinsamkeiten und Unterschiede der gewählten Kommunikationsstrategien im Rahmen der untersuchten fünf Anwendungsszenarien führt zu der Identifikation dreier unterschiedlicher Herangehensweisen in der Vermittlung des neuen Angebots an die Bürger. Diese drei Herangehensweisen können insbesondere anhand der Einbindung unterschiedlicher Partner sowie deren Rollen in der Kommunikation mit dem Bürger unterschieden werden.

Die folgenden drei Strategien (s. Abbildung 39) werden unterschieden:

(1) Drittpartei-Strategie,
(2) Dezentrale Strategie,
(3) Zentrale Strategie.

Sie sollen im Folgenden skizziert werden.

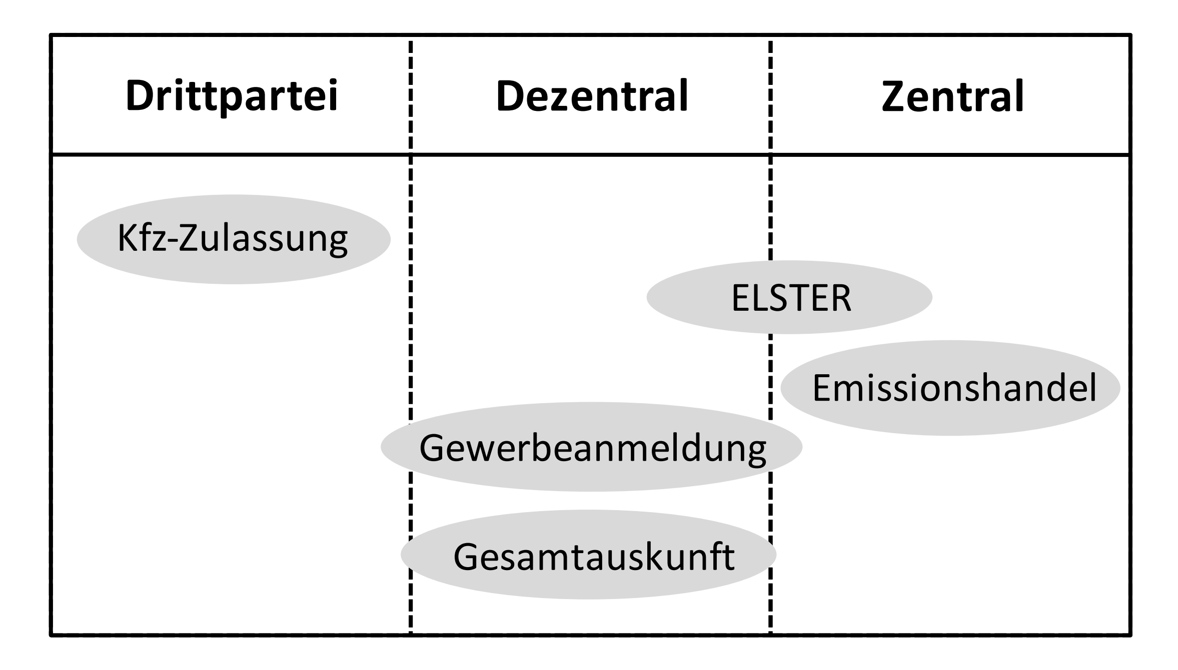


Abbildung 39: Differenzierung von drei Kommunikationsstrategien

5.3.1.Differenzierung der Kommunikationsstrategien

5.3.1.1. *Zentrale Strategie*

Im Falle der "zentralen" Strategie wird das Angebot durch eine spezifische Behörde angeboten. Sie bietet den relevanten Zugangsweg an, stellt also so etwas wie einen "One-Stop-Shop" dar. Entsprechend übernimmt die Behörde weitgehend im Alleingang die Kommunikation mit den Nutzern und orientiert diese über die Verfügbarkeit und den Nutzen des Angebots.

Ein Beispiel für diese Strategie ist der hier betrachtete Fall Emissionshandel, bei dem die DEHSt als alleiniger Anbieter auftritt, den Zugangsweg zum Angebot stellt und die Information der Nutzer übernimmt. Auch der Kundendienst wird hier zentral übernommen.

5.3.1.2. *Dezentrale Strategie*

Im Falle der "dezentralen" Strategie findet eine Arbeitsteilung zwischen einem Anbieter des Dienstes (häufig als reiner Backend-Anbieter) und einer Vielzahl behördlicher Vermittler (Frontend) statt. Während der Anbieter hier zwar Informationen oder Materialien für die Kommunikation an die Endnutzer vorbereiten kann, liegt die tatsächliche Vermittlung in der Hand der Behörden mit Kundenkontakt.

Beispiele für diese Strategie sind die Gewerbeanmeldung, die Gesamtauskunft, und (weitgehend) ELSTER. Der Zugangsweg zum Angebot erfolgt hier über die lokalen Gewerbe-, Melde-, oder Finanzämter, wie auch schon im Rahmen des traditionellen physischen Angebots. Die Anbieter im Hin-

tergrund (DZBW, AKDB, AG) stellen zwar die Infrastruktur und elektronische Abwicklung, in gewissem Masse auch Kundeninformationen zur Verfügung, bleiben bei der Vermittlung jedoch wenig prominent. Auch der Kundendienst im Falle von Problemen oder Fragen zum Angebot wird weiterhin über die lokalen Ämter angeboten und abgewickelt.

5.3.1.3. *Drittpartei-Strategie*

Im Falle der "Drittpartei"-Strategie kooperieren behördliche Anbieter mit privaten. Dabei stellen die privaten Anbieter den Zugang zum behördlichen Angebot dar, indem sie den behördlichen Prozess in ihr kommerzielles Angebot einbinden. Entsprechend übernehmen die privaten Kooperationspartner, oder eben Drittparteien, die Vermittlung des Angebots an die Kunden.

Als Beispiel für diese Strategie darf im Rahmen der hier beschriebenen Erhebung die Kfz-Anmeldung gelten. Die Vermittlung des Prozesses geschieht dabei durch die privaten Kooperationspartner Autohaus und Dienstleister. Diese sind es, die am Point of Sale mit den Kunden in Kontakt treten. Im Falle des Pilotprojektes sind sogar Kundendienstmitarbeiter vor Ort, welche die Bedienung und Abwicklung des Prozesses übernehmen und so Zugangshürden abbauen.

Im Falle von Fragen und Beschwerden stellen im Rahmen dieser Strategie ebenfalls die privaten Kooperationspartner die ersten Zugangsstellen dar, würden sich jedoch gegebenenfalls ihrerseits an den behördlichen Anbieter im Hintergrund wenden müssen.

5.3.2. Vergleich der Kommunikationsstrategien

Die drei beschriebenen generalisierten Kommunikationsstrategien unterscheiden sich hinsichtlich ihrer Vorteile wie auch Herausforderungen (s. Abbildung 40). Sie sind entsprechend unterschiedlich geeignet für verschiedene Anwendungskontexte.

Die "zentrale" Strategie zeichnet sich durch eine hohe Kontrolle der zuständigen Behörde über alle Elemente und Schritte des Kommunikationsprozesses aus. Der koordinative Aufwand beschränkt sich auf die behördeninterne Abstimmung. Entsprechend fällt es in diesem Szenario leicht, einen konsistenten Aussenauftritt sicherzustellen. Die inhaltliche Zusammenstellung wie auch Gestaltung der gewählten Instrumente, die Bereitstellung von Ansprechpartnern und eines Kundendienstes liegen alle in der Hand der Behörde. Auf der anderen Seite ist es jedoch auch allein Aufgabe der Behörde, die relevanten Zielgruppen zu erreichen. Als ein Kommunikator unter zahllosen weiteren kann es hier also durchaus eine Herausforderung darstellen, eine ausreichende Aufmerksamkeit unter den Zielpersonen zu gewinnen.

Die "dezentrale" Strategie entlastet die verantwortliche Stelle von der direkten Kommunikation mit den Zielpersonen. Der Austausch findet hier über behördliche Kooperationspartner bzw. lokale Repräsentanten statt. Entsprechend bestehen erhöhte Anforderungen hinsichtlich der Kooperation und Koordination der Beteiligten. Die Vielfalt in der Aussendrastellung nimmt zu, die Sicherstellung eines einheitlichen Aussenauftritts wird erschwert. Nachdem der Koordinationsprozess jedoch auch hier verwaltungsintern abläuft, und somit gewisse gemeinsame Spielregeln und definierte Abläufe und Prozesse vorliegen, ist der Koordinationsaufwand als moderat zu beurteilen. Eine Herausforderung ist dagegen zweifellos die Überwachung oder Einhaltung definierter Standards in der Zielgruppenansprache: Werden die Schnittstellen einheitlich gestaltet? Werden einheitliche Instrumente verwendet? Wird ein gemeinsames Niveau im Kundendienst sichergestellt? Legen alle Beteiligten ein ähnliches Engagement bei der Vermittlung des Angebots an den Tag? Vor allem letzteres kann aufgrund der Autonomie der eingebundenen lokalen Stellen keineswegs vorausgesetzt werden. Ein Vorteil dieser Strategie liegt dagegen zweifellos darin, dass einer breiten Nutzerbasis lokale Ansprechpartner angeboten werden, eine breite Vertretung des Angebots in der Fläche des Landes kann so erreicht werden.

Die "Drittpartei"-Strategie erhöht einerseits die Dynamik des Kommunikationsprozesses, ist jedoch auch mit einer grösseren Vielfalt und einem gesteigerten Koordinationsbedürfnis verbunden. Die Einbindung des behördlichen Angebots in kommerzielle Prozesse stellt sicher, dass die beteiligten Parteien über ein hohes Interesse an der Vermarktung des Angebots verfügen, entsprechend kann das Engagement der kommunizierenden Parteien gestärkt werden. Durch die Einbindung unterschiedlicher privater Akteure wird die Angebotsvermittlung auf eine breite Basis gestellt, Synergieeffekte in der Nutzerwahrnehmung können so erzielt werden. Die beteiligten Parteien können eine grosse Kreativität in der Zielgruppenansprache entfalten, was erneut die zuständige Behörde von entsprechenden Bemühungen entlastet. Ebenso kann der Kundendienst in einem ersten Schritt an die privaten Kooperationspartner delegiert werden. Auf der anderen Seite wird es der Behörde erheblich erschwert, eine Einheitlichkeit und Konsistenz im Aussenauftritt sicherzustellen. Die Koordination, vor allem mit einer Vielzahl privater Kooperationspartner, kann durchaus mit einem beträchtlichen Aufwand verbunden sein.

		Drittpartei	Dezentral	Zentral
Kommunikationsprozess	Kooperation	+++	++	-
	Kontrolle	-	+	+++
	Einheitlichkeit	-	+	+++
	Vielfalt	+++	++	+
	Synergien	+++	++	-
Angebot	Innovation	+++	+	+/+++
	Breite	++	+++	-
	Private Nutzung	+++	+	++

Abbildung 40: Vergleich der Kommunikationsstrategien

Soll eine breite Vielzahl an Nutzern von einem innovativen Angebot überzeugt werden, so eignet sich insbesondere eine Drittpartei-Strategie. Diese Strategie entfaltet die grösste Dynamik und Vielfalt in der Aussendarstellung. Nutzer können auf unterschiedliche Weisen, zahlreichen Kanälen und durch mehrere Akteure angesprochen werden. Die Botschaft wird durch deren Aussenauftritte und Marken gestützt. Eine professionelle Gestaltung der Kommunikation sowie gewisse Standards des Kundendienstes werden gefördert.

Soll eine breite Nutzerbasis angesprochen werden, jedoch im Rahmen weniger neuartiger Angebote, oder im Falle obligatorischer Prozesse, so ist vor allem die dezentrale Strategie geeignet, ein flächendeckendes Angebot sicherzustellen. Hier kann ein zentraler Anbieter die Vertriebskraft lokaler Aussenstellen nutzen, sofern diese gut geschult und effizient eingebunden werden. Eine gewisse Vielfalt in der Aussendarstellung sowie den Serviceniveaus ist dabei unvermeidlich.

Handelt es sich um ein Angebot im Kontext sehr spezifischer Geschäftsvorfälle, insbesondere im Falle eines B-2-G-Angebots, so ist besonders eine zentrale Kommunikationsstrategie geeignet. Sie eignet sich für Angebote unterschiedlicher Innovationsgrade. Es können hier relevante Botschaften konzentriert, einheitlich und zielgenau an die definierte Zielgruppe vermittelt werden. Dabei wird zwar eine grosse Breitenwirkung der Kommunikation erschwert (bzw. sie fordert der Behörde erhebliche Ressourcen ab), gleichzeitig steigt aber die Kontrolle über Qualität und Eigenschaften des Angebots. Der Koordinationsaufwand kann zugunsten eine fokussierten Angebots reduziert werden.

Die Spanne der eingesetzten Instrumente ist über alle drei beschriebenen Strategien hinweg breit. Auch hier entfaltet die Drittpartei-Strategie eine grosse Dynamik und Vielfalt. Unterschiedliche Partner gestalten hier Instrumente nach ihren jeweiligen Standards und Interessen. Professionelle Marketingmassnahmen, zugeschnitten auf ein spezifisches Angebot, sind hier möglich und wahrscheinlich. Nutzer können über eine Vielzahl unterschiedlich gestalteter Aussenstellen kontaktiert werden. Im Falle der dezentralen Strategie ist dagegen eher von einer "stillschweigenden Integration" neuer Angebote zu rechnen. Die beteiligten lokalen Behörden erneuern oder erweitern lediglich ihr Angebot, bestehende Prozesse werden hier ergänzt. Die Wahrscheinlichkeit, dass das neue Angebot eigenständig beworben wird, ist geringer. Im Falle der zentralen Strategie ist eine "stillschweigende Integration" des neuen Angebots in bestehende Prozesse ebenso möglich, wie eine offensive Vermarktung durch eigens gestaltete Instrumente. Die verantwortliche Behörde verfügt hier über eine grössere Freiheit bei der Gestaltung von Instrumenten und Kanälen, als dies bei der dezentralen Strategie der Fall ist, welche eine erhöhte Koordination erfordert.

Beispiel ELSTER

Unter den hier analysierten Anwendungskontexten stellt vor allem der Fall ELSTER ein interessantes Anschauungsbeispiel für die Kombination unterschiedlicher Strategien und die Nutzung ihrer unterschiedlichen Vorteile dar: Für unterschiedliche Elemente des Kommunikationsprozesses (Web-Auftritt, Marketing) wurden führende Verantwortliche definiert. Diese verbindet ein gemeinsames Interesse an einem einheitlichen, professionellen Aussenauftritt. Die Kommunikation des Prozesses zeichnet sich entsprechend durch eine hohe Einheitlichkeit im Design, ein gemeinsames Logo, die Etablierung einer wiedererkennbaren Marke, einen einheitlichen Kundendienst, eine konsistente Farbführung und die Erstellung professionell gestalteter Materialen aus. Die Verantwortlichen geniessen die Freiheit und Eigenverantwortung, welche vor allem die zentrale Kommunikationsstrategie auszeichnet.

Dennoch wurde in der Vermittlung des Angebots an die Nutzer eine dezentrale Strategie gewählt, was vor allem angesichts der Breite der angestrebten Nutzerbasis als sinnvoll betrachtet werden kann. Da ein bestehender Prozess durch ein e-Government-Angebot ergänzt wird, wurde dabei auf eine Drittpartei-Strategie weitgehend verzichtet. Auch von dieser lassen sich jedoch Elemente finden, da etwa die ELSTER-Prozesse in kommerzielle Software-Angebote intergiert wurden. Ein Schwerpunkt in der Vermittlung liegt jedoch auf den lokalen Finanzämtern. Diesen wird zentral eine Auswahl an Kommunikationsmaterialien bereitgestellt, welche auf den spezifischen Vermittlungskontext selektiv angepasst werden können. Die Koordination mit den Aussenstellen und vor allem auch deren Einbindung und Motivation wird sichergestellt, indem lokale Botschafter des Angebots identifiziert werden, für die eigens Informationsmaterialien und Schulungsangebote bereitstehen. Mögliche Nachteile der dezentralen Strategie, wie eine mangelnde Dynamik, Motivation oder Einheitlichkeit des Angebots werden so reduziert. Damit steigt zwar auch der Koordinationsaufwand des Projekts, für den Anwen-

dungskontext eines C-2-G-Angebots mit breiter Nutzerbasis und moderatem Innovationsgrad kann jedoch von einer beispielhaft durchdachten und implementierten Strategie gesprochen werden, welche offenbar auch einen grossen Erfolg in der Vermittlung an die Nutzer erzielen konnte.

6. Zusammenfassung und Handlungsempfehlungen

6.1. Markteinführungsstrategie für eID-Infrastrukturen

These 1: Nur die Kombination aus Infrastruktur und Angeboten bringt Nutzen

These 2: Kenntnisse und Nutzung von Netzeffekten sind ausschlaggebend für den Einführungserfolg

These 3: Zielgruppenorientierung und Marketing sind zentrale Erfolgsfaktoren

Im vorliegenden Projektbericht wurde zunächst auf die theoretischen Erkenntnisse von Vertrauen, Risiken und Akzeptanzfaktoren aus der Literatur zurückgegriffen. Im nächsten Schritt wurden Markteinführungsstrategien und Geschäftsmodelle betrachtet. Um die theoretischen Erkenntnisse zu stützen, wurden aus den Anwendungstests Szenarien ausgewählt, die näher analysiert wurden.

Der nPA wurde zwar Ende 2010 eingeführt und das klassische ‚Henne-Ei-Problem‘ zwischen Chipkarten und Anwendungen scheint dadurch gelöst, da Bürger im Laufe der Zeit den nPA besitzen werden, da von Behörden keine anderen Ausweise mehr ausgestellt werden. Derzeit können aber nur wenige Dienstleistungen vollständig elektronisch mithilfe des nPA abgewickelt werden, da Behörden derzeit nur sehr wenige Dienstleistungen für den nPA anbieten. Ein weiteres Problem besteht aber weiterhin im Hinblick auf die Verbreitung der optionalen qualifizierten Signatur. Von Seiten der Dienstleistungsanbieter gilt es etwaige zum Teil technische Probleme noch zu beseitigen und das Dienstleistungsangebot auszuweiten. Erst wenn Behörden das Dienstleistungsangebot erweitern, werden Bürger diese nutzen, was wiederum Vorteile sowohl für Behörden als auch für Bürger mit sich bringt.

Des Weiteren betreffen aktuell vorgebrachte Bedenken, nachdem der nPA nicht sicher genug sei oder die obligatorische PIN ausgeforscht werden kann, nur die Nutzung von unsicheren Endgeräten. Aus diesem Grund wird von Experten empfohlen den nPA nur in Kombination mit Kartenlesegeräten der Sicherheitsstufe drei zu verwenden. Wenn PINs mangels PIN-Pad und Visualisierung im Kartenleser über die Tastatur eines Rechners eingegeben werden müssen, hängt die Sicherheit der Transaktion von der Sicherheit des Rechners ab. Die Sicherheit der Rechner ist sehr wichtig, da es nahezu unmöglich ist einen Vorgang sicher durchzuführen, wenn Angreifer Rechner, Tastatur und Bildschirm unter Kontrolle gebracht haben.

Zu den Akzeptanz fördernden Schritten der eID-Funktion des nPA zählen nach Expertenmeinungen eine gute Promotion des nPA mit Marketingmaßnahmen und bürgerfreundliche Erklärungen der neuen Funktionen, sowohl im Meldeamt als auch in der Öffentlichkeit. Die Angebotsbreite der Anwendungen im Internet sind laut Expertenmeinungen ebenso entscheiden für die Akzeptanz der eID-Funktion.

Mit dem nPA gibt es erstmals ein Instrument, mit dem man seine Identität jederzeit – offline wie auch online – selbstbestimmt, transparent und sicher dokumentieren kann. Hinsichtlich der Sicherheitsaspekte sind sowohl Hersteller – insbesondere das BSI – in der Pflicht Aufklärung über Restrisiken zu leisten. Denn technisch machbare, wirtschaftlich profitable und rechtlich konforme Sicherheitslösungen können nur durch konstruktive Zusammenarbeit von Technologie, Wirtschaft und Regulierung erfüllt werden (o. V. 2010c, 90ff).

6.2. Kommunikationsstrategie für eID-Infrastrukturen

These 4: Je neuartiger und komplexer ein Angebot, desto aufwändiger ist dessen kommunikative Vermittlung.

These 5: Die Einbindung lokaler Behörden erleichtert die flächendeckende Ansprache einer breiten Nutzerbasis.

These 6: Die Kooperation mit privaten Anbietern erzeugt Vielfalt und Synergie-Effekte in der Kommunikation.

Die kommunikative Vermittlung von eID-Infrastrukturprojekten ist keine "one size fits all"-Aufgabe. Wenngleich in jedem Fall ein zentrales Ziel darin erkannt werden kann, die Akzeptanz der Nutzer und relevanten Kooperationspartner zu gewinnen, sind zahlreiche Einflussfaktoren bei der Wahl einer angemessenen Kommunikationsstrategie zu berücksichtigen. Basierend auf theoretischen Vorerkenntnissen wurden in diesem Bericht insbesondere innovations- und nutzerbezogene Einflussfaktoren der Einführung von eGovernment-Angeboten vorgestellt. Die darauf aufbauende Analyse und Differenzierung von Kommunikationsstrategien, basierend auf den fünf betrachteten Anwendungskontexten, spiegeln ebenfalls diese Einflussfaktoren wieder. Bei der Wahl einer Kommunikationsstrategie ist also die Frage zu stellen, welchen Innovationsgrad ein Angebot aufweist - damit verbunden auch die Fragen, welche relativen Vorteile, welche Komplexität, welche Kompatibilität mit einem Angebot verbunden sind. Ist das Angebot neuartig, ist es kompliziert zu bedienen, ist es mit hohen (auch finanziellen) Aufwänden und Ein- oder Umstiegshürden verbunden? Je neuartiger ein Angebot erscheint, desto höher ist das mit der Nutzung verbundene subjektive Risiko der Zielgruppen. Und desto aufwändiger ist die kommunikative Erzeugung von Vertrauen und Akzeptanz.

Neben den innovationsbezogenen Einflussfaktoren sind immer auch Fragen nach den Charakteristika der Zielgruppen zu stellen. Wir hatten festgestellt, dass im Rahmen von eID Infrastrukturprojekten nicht allein Anbieter und Nachfrager ein tragende Rolle spielen - auch weitere Anspruchsgruppen wie Mitarbeiter, Kooperationspartner, Medien und andere Intermediäre tragen zum Erfolg von Implementationsstrategien bei, und sollten im Rahmen der kommunikativen Bemühungen berücksichtigt werden. Die vorliegende Analyse konzentrierte sich dabei auf die direkte und indirekte Ansprache der

Nutzer durch die Anbieter. Alleine hier ist eine grosse mögliche Vielfalt der Austauschbeziehungen zu beobachten: Handelt es sich um eine breite oder stark eingeschränkte Nutzerbasis? Findet die Nutzung in einem privaten oder beruflichen Kontext statt? Sind soziodemographische Einschränkungen zu beachten? Von welchen Nutzungsbefähigungen kann ausgegangen werden? Gerade wenn Vertrauen und Akzeptanz als subjektive Einstellung verstanden werden, ist die Bedeutung nutzerbezogener Einflussfaktoren evident.

Neben Einflussfaktoren des Angebots und der Nutzer besteht eine Reihe von Kontextfaktoren, die ebenfalls bei der Wahl einer Kommunikationsstrategie betrachtete werden sollten - so entfalten die Verfügbarkeit einer öffentlichen Infrastruktur, das kulturelle und mediale Umfeld zweifellos Wirkung auf die Annahme oder Ablehnung eines neuen Angebots durch die Zielpersonen. In der vorliegenden Analyse wurden diese Elemente nicht vertieft betrachtet, da von einer deutschlandweiten Vergleichbarkeit dieser Kontextfaktoren ausgegangen wurde. Diese Voraussetzung ändert sich jedoch, wenn ein Angebot kulturell und infrastrukturell vielfältigere Märkte adressiert.

E-Government-Angebote zeichnen sich in der Regel dadurch aus, dass die Adressierung der Zielgruppen online, also elektronisch vermittelt geschieht. Die bedeutendste Kommunikationsplattform ist der Webauftritt des Angebots. Hier wird auch die weit überwiegende Mehrzahl der Daten und Informationen bereitgehalten und vermittelt. Kommunikationsstrategien für eID-Infrastrukturprojekte haben sich jedoch keineswegs alleine auf die Online-Kommunikation zu beschränken. Eine Vielzahl weiterer Kanäle steht für die Ansprache der Zielgruppen zur Verfügung: Briefe, Prospekte, Plakate, Rundfunkauftritte, Messen, und nicht zuletzt die persönliche Betreuung durch einen Kundendienst oder die anbietenden Ämter werden in der Kundenkommunikation eingesetzt. Die Theorie gibt zu bedenken, dass Online-Transaktionen stets medial vermittelt sind und daher den Aufbau vertrauensstiftender persönlicher Beziehungen erschweren. Insbesondere ein Kundendienst kann dem entgegenwirken, stellt jedoch andererseits immer auch einen prozessverlängernden Medienbruch dar. Noch scheinen die vielfältigen Interaktionsmöglichkeiten des (sozialen) Internets nicht für die Implementation von eGovernment-Angebote erschlossen worden zu sein. Ein befragter kommerzieller Anbieter brachte immerhin die Möglichkeit des Suchmaschinenmarketings ins Spiel. Weitergehende Angebote, wie Foren, Blogs oder Chats, spielten dagegen bisher noch keine Rolle im Rahmen der untersuchten Kommunikationsstrategien.

Die Tonalität von Kommunikationsstrategien kann eine grosse Bandbreite aufweisen. In den untersuchten Kontexten wurde in der Regel eine sachlich-informative Ansprache der Zielgruppen bevorzugt. Im Falle des ELSTER-Angebots spielten jedoch auch emotional-spielerische Elemente eine Rolle, etwa in Form eines Gewinnspiels oder eines "Maskottchens". Die Vertrauensforschung legt grossen Wert auf transparente und faire Kommunikation zwischen Anbieter und Nutzer. Eine umfassende Bereitstellung relevanter Informationen soll die Beurteilung eines Angebots erleichtern und so Vertrauen erzeugen. Neben der Reduktion von Sorgen kann jedoch auch der gezielte Aufbau von Vertrauen

durch eine entsprechende Pflege der Anbieterreputation angestrebt werden. Dies ist üblicherweise die Aufgabe eines professionellen Marketings, wie es bei privatwirtschaftlichen Angeboten üblich ist. Erneut lassen sich Elemente dieses Ansatzes im Fallbeispiel ELSTER beobachten, wo die Etablierung einer wiedererkennbaren Marke angestrebt wird. Eine emotional-spielerische Tonalität in der Nutzerkommunikation ist vor allem dort wahrscheinlicher, wo eine breite Nutzerbasis angesprochen werden soll, wo ein privater Nutzungskontext vorliegt und wo privatwirtschaftliche Akteure in das Angebot eingebunden werden.

Die vorliegende Analyse konnte insbesondere drei Kommunikationsstrategien unterscheiden, welche in den untersuchten Anwendungskontexten zum Tragen kamen: eine "zentrale" Strategie liegt dann vor, wenn eine anbietende Behörde direkt und gezielt ihre Zielgruppe adressiert und damit die Hoheit über die Gestaltung der Kommunikationsbemühungen besitzt. Eine "dezentrale" Strategie bindet dagegen eine Vielzahl behördlicher Kooperationspartner ein - der Anbieter bleibt weitgehend im Hintergrund und stellt Infrastrukturen, Informationen und gegebenenfalls auch Materialien zur Verfügung, lokale Behörden adressieren jedoch gleichsam als "Aussenstellen" direkt die betroffenen Zielgruppen. Die "Drittpartei"-Strategie bindet schliesslich privatwirtschaftliche Kooperationspartner in die Zielgruppenansprache ein, wobei eine grosse Vielfalt an beteiligten Parteien und Austauschverhältnissen denkbar ist.

Wir konnten feststellen, dass sich die "zentrale" Strategie durch eine hohe Kontrolle des Anbieters über den Kommunikationsprozess und dadurch eine hohe potentielle Einheitlichkeit des Aussenauftritts auszeichnet. Die "dezentrale" Strategie weist die Stärke einer hohen Flächenpräsenz und möglichen persönlichen Ansprache der Zielgruppen auf, während die Koordination und Kontrolle des Prozesses erschwert wird, die Einheitlichkeit des Auftrittes tendenziell abnimmt. Die "Drittpartei"-Strategie weist schliesslich hohe Synergie-Potentiale auf, wenn zahlreiche unterschiedliche Kooperationspartner gemeinsam und auch unabhängig voneinander die Zielgruppen mit ihren Botschaften adressieren und diese dabei durch ihre jeweilige Glaubwürdigkeit stützen. Auch ist hier von einer hohen Dynamik und Vielfalt der Kommunikationsbemühungen auszugehen, wenn die beteiligten Parteien kommerzielle Interessen mit dem Erfolg des Angebots verbinden - die anbietende Behörde hat jedoch umgekehrt in diesem Fall die Kontrolle über den Kommunikationsprozess weitgehend aufzugeben und ist gegebenenfalls mit einem erheblichen Koordinationsaufwand konfrontiert.

Welche innovations- und nutzerbezogenen Einflussfaktoren sprechen nun jedoch für die Wahl der einen oder anderen Strategie? Ist das Angebot mit einem hohen Neuigkeitsgrad verbunden, sind also nicht unerheblich Einstiegs- und Umstellungshürden zu erwarten, so weisen die zentrale und Drittpartei-Strategien Vorteile auf: im Falle der zentralen Strategie können die Eigenschaften des Angebots sachlich, umfassend und einheitlich aufgezeigt und erklärt werden, im Falle der Drittpartei-Strategie entwickeln die Dynamik und Vielfalt der Kommunikatoren und ihrer Massnahmen ein hohes Überzeugungspotential. Im Falle der dezentralen Strategie bestünde eine Herausforderung darin, sicherzu-

stellen, dass das Angebot tatsächlich mit ausreichender Überzeugung und Sachkenntnis flächendeckend kommuniziert wird. Soll eine breite Nutzerbasis angesprochen werden, so weisen die dezentrale sowie die Drittpartei-Strategien Stärken auf, da sie eine grössere Anzahl an Kommunikatoren einbinden und eher eine flächendeckende Kommunikation sicherstellen können.

Angebote für einen privaten Nutzungskontext und gegebenenfalls emotional-spielerische Kommunikationsansätze sind vor allem geeignet für den Fall einer Drittpartei- sowie, in geringerem Masse, eine zentrale Strategie. Privatwirtschaftliche Akteure weisen in der Regel eine grössere Erfahrung in der Vermarktung von Angeboten für einen privaten Nutzungskontext auf und können diese durch ihre Markenauftritte untermauern. Die Dynamik und Vielfalt der Drittpartei-Strategie enthalten Potentiale für die Generierung von Ideen und Ansätzen für eine spielerische Ansprache der Zielgruppen. Im Falle der zentralen Strategie kann eine solche jedoch ebenfalls gezielt entwickelt, möglicherwiese beauftragt werden. Die dezentralen und zentralen Strategien sind besonders geeignet für eine sachliche und informationsbezogene Ansprache der Zielgruppen, wie sie vor allem auch in einem professionellen oder beruflichen Kontext eine Rolle spielen. Im Falle der zentralen Strategie kann der Anbieter die Kontrolle über eine sachliche Informationsleistung sicherstellen und eine einheitliche Schnittstelle vor allem auch für betriebliche Nutzer gestalten. Im Falle der dezentralen Strategie kann durch eine entsprechende Informationsbereitstellung und Schulung erreicht werden, dass die behördlichen Kooperationspartner den Nutzern kompetente Auskunft und Unterstützung bieten. Eine sachlich korrekte Kommunikation ist hier einfacher sicherzustellen, als eine emotionale Überzeugungsarbeit.

Strategien sind naturgemäss kontingent. Sie hängen ab von Eigenschaften des Anbieters, des Angebots, der Zielgruppen und verschiedenster Rahmenbedingungen. Dies gilt auch für Kommunikationsstrategien im Rahmen von eID-Infrastrukturprojekten. Die vorliegende Analyse soll einen Überblick bieten, welche Strategien für die Vermittlung eines innovativen Angebots denkbar und für welchen Kontext besonders angemessen sein können. Die Wahl einer angemessenen Kommunikationsstrategie erhöht die Wahrscheinlichkeit, dass erfolgreich Vertrauen aufgebaut und Akzeptanz geschaffen werden kann - ganz gleich ob in einem privaten oder betrieblichen Kontext, bei einer sehr spezifischen oder einer sehr breiten Zielgruppe, im Falle sehr komplexer oder wenig herausfordernder Innovationen. Die vielfältigen Anwendungskontexte des nPA bieten umfangreiches Anschauungsmaterial, aus dem zahlreiche Lehren für eine mehr oder weniger geschickte Kommunikation von eGovernment-Angeboten gezogen können, die zweifellos weit über die hier aufgeführten hinausgehen. Sie sollten daher weiterhin mit Aufmerksamkeit beobachtet und analysiert werden.

ANHANG

A. Risiken und mögliche Gegenmaßnahmen für den Missbrauch von digitalen Ausweisen bei E-Government Dienstleistungen

Risiko	Mögliche Gegenmaßnahmen
R1) fiktive, reale Identität Ein Kunde erhält einen Berechtigungsnachweis, der sich auf eine fiktive reale Identität bezieht.	Mögliche Gegenmaßnahmen, um vor der Ausgabe des Berechtigungsnachweises sicherzustellen, dass eine reale Identität existiert, umfassen: C1a) Vergleich der Angaben mit Melderegistern oder Aufzeichnungen der Organisation C1b) Vorgaben, dass eine vertrauenswürdige Person bzw. Organisation die angegebenen Informationen bestätigt C1c) Kontrolle von originalen Dokumenten
R2) falsche Angaben Falsche Informationen zu einer echten, realen Identität werden gespeichert und daraufhin wird diesen Glauben geschenkt.	Mögliche Gegenmaßnahmen, um sicherzustellen, dass Merkmale, die während des Registrierungsprozesses angegeben wurden, korrekt sind, umfassen: C2a) Vergleich der Angaben mit Melderegistern oder Aufzeichnungen der Organisation C2b) Vorgaben, dass die sich registrierende Person die Korrektheit seiner Angaben bescheinigen muss C2c) Vorgaben, dass eine vertrauenswürdige Person bzw. Organisation die angegebenen Informationen bestätigen muss
R3) Diebstahl des Zugangstokens Ein Zugangstoken, der eine Zugangsberechtigung beinhaltet, wird vom oder auf dem Weg zum Nutzer gestohlen. Er wird entweder direkt zur Authentifizierung von einem Betrüger benutzt oder wird verwendet um Informationen über den Nutzer für spätere Missbräuche zu erhalten	Mögliche Maßnahmen zur Reduktion des Diebstahlrisikos umfassen: C3a) Vorgaben, dass der Zugangstoken nur unter Nutzung angemessener Kurierdienstleistungen ausgeliefert oder nur persönlich an den registrierten Nutzer ausgegeben wird C3b) Sicherstellung, dass ein Zugangstoken nur in Verbindung mit PIN, Passwort, Biometrie oder einer anderer Methode zur Nutzerprüfung verwendet werden kann. Alle geheimen Daten, die für die Nutzung während des Verifikationsprozesses vorgesehen sind, sind separat vom Token selbst zu liefern, auszugeben oder müssen sicher im Token gespeichert sein C3c) Sicherstellung, dass ein Minimum von öffentlichen Daten in zugreifbarer Form auf dem Token gespeichert sind
R4) Diebstahl der realen Identität Eine wahre reale Identität wird zum Zeitpunkt der Registrierung veruntreut.	Mögliche Maßnahmen, um sicherzustellen, dass Berechtigungsnachweise nur an den wahren Vertreter dieser realen Identität ausgegeben werden, umfassen: C4a) Überprüfung von originalen Dokumenten zum

	Zeitpunkt der Registrierung C4b) Fragen an die sich registrierende Person, die von nicht veröffentlichten Informationen über den Vertreter der realen Identität abgeleitet wurden C4c) Vorgaben, dass eine vertrauenswürdige Person bzw. Organisation für die sich registrierende Person bürgt C4d) Kontaktaufnahme mit der vermeintlichen, sich registrierenden Person über den eingetragenen Wohnsitz oder die Telefonnummer C4e) Entsendung des Berechtigungsnachweises nur an den eingetragenen Wohnsitz des Vertreters der realen Identität
R5) Abfangen oder Enthüllen von geheimen Authentifizierungsinformationen Geheime Informationen (wie z. B. PIN oder privater Unterschriftsschlüssel) werden bei der Übertragung der Zugangsberechtigung abgefangen, von einem E-Government Nutzer aufgerufen oder durch den Nutzer oder eine andere Partei absichtlich oder versehentlich enthüllt	Mögliche Maßnahmen zur Reduzierung des Abfangs- oder Enthüllungsrisikos geheimer Authentifizierungsinformationen, umfassen: C5a) Sicherstellung, dass geheime Informationen überhaupt nicht übermittelt werden, z. B. durch die Nutzung einer Smart Card, bei der der private Schlüssel den Token nie verlässt, um Informationen zu unterzeichnen oder zu verschlüsseln C5b) Sicherstellung, dass geheime Informationen nur in verschlüsselter Form, über einen verschlüsselten Kanal oder über eine von Natur aus sichere Kommunikationsleitung übertragen werden C5c) Sicherstellung, dass geheime Informationen unverschlüsselt nicht im Ganzen übermittelt werden; z. B.: Bei einem Vorgang in einem Callcenter wird der Kunde nur nach einem oder mehreren Zeichen aus einer Reihe von geheimen Nummern und/oder Phrasen gefragt. Der Telefonist sollte auch nur Zugang zu diesen einzelnen Zeichen haben C5d) Nutzung von eher dynamischen als statischen Informationen, so ist z. B. bei der Verifikation der Identität durch ein Callcenter die Frage an den Anrufer über kürzlich erfolgte Transaktionen verlässlicher als die Frage nach der Kontonummer oder den Mädchennamen der Mutter, die durch einen Betrüger herausgefunden worden sein können C5e) Abschluss einer vertraglichen Verpflichtung, dass der Nutzer keine geheimen Authentifizierungsinformationen enthüllt
R6) Aufbewahrung von geheimen Authentifizierungsinformationen in einem nicht vertrauenswürdigen Terminal Geheime Informationen werden von einer nicht vertrauenswürdigen Datenstation aufbewahrt (wie z. B. Heim- oder Arbeits-PC, PC in einem Internetcafé oder öffentlichen Kiosk). Solche geheimen Informationen umfassen z. B. private Signaturschlüssel, die	Gegenmaßnahmen für dieses Risiko müssen technologiespezifisch sein, aber könnten Folgendes umfassen: C6a) Sicherstellung, dass Geheimnisse nicht in einer vertrauensunwürdigen Umgebung gespeichert, sondern komplett in einem vertrauenswürdigen Token aufbewahrt werden, wie z. B. in einer Smart Card, die für die Ausführung des Signaturvorgangs

für die Ausführung von kryptografischen Funktionen innerhalb des Terminals benutzt wurden und PINs, die in ein webbasiertes Formular eingegeben wurden und daraufhin im Pufferspeicher gehalten werden	programmiert wurde C6b) Sicherstellung, dass Geheimnisse ordnungsgemäß beaufsichtigt und hundertprozentig entsorgt werden, wenn Sie nicht mehr gebraucht werden
R7) Nicht genehmigte Nutzung von Zugangstoken Ein Zugangstoken wird von einem anderen Anwender, als der an den er ausgegeben wurde, genutzt	Maßnahmen gegen die nicht genehmigte Nutzung eines Zugangstokens umfassen: C7a) Vorgaben, dass Authentifizierungsgeräte durch ein Nutzerprüfungssystem, das z. B. Passwort, PIN oder Biometrie verwendet, geschützt werden
R8) Nutzung von kompromittierten Berechtigungsnachweisen Ein Berechtigungsnachweis wird, nachdem er kompromittiert wurde, benutzt	Mögliche Gegenmaßnahmen für die Nutzung von kompromittierten Berechtigungsnachweisen umfassen: C8a) Ermöglichung und Ermutigung der Kunden und der vertrauenswürdigen Parteien verdächtigte Störung an einen Helpdesk Dienst, der dauerhaft verfügbar ist, zu melden C8b) Begrenzung der Lebensdauer von Berechtigungsnachweisen auf eine bestimmte Zeit C8c) Es wird den vertrauenswürdigen Parteien ermöglicht die Gültigkeit eines Berechtigungsnachweises in Bezug auf eine Berechtigungsnachweissperrliste während der Nutzung zu überprüfen C8d) Es wird den vertrauenswürdigen Parteien ermöglicht eine positive Bestätigung der Gültigkeit eines Berechtigungsnachweises während der Nutzung mithilfe eines Autorisierungsprozesses zu erhalten
R9) Nutzung eines Berechtigungsnachweises nach wesentlicher Veränderung der Umstände Ein Berechtigungsnachweis wird verwendet, obwohl eine Veränderung der Umstände eingetreten ist, dies bedeutet, dass der Berechtigungsnachweis normalerweise nicht ausgestellt worden wäre	Mögliche Maßnahmen, um vor der Nutzung eines Berechtigungsnachweises nach einer wesentlichen Veränderung der Umstände zu schützen, umfassen: C9a) Vertragliche Verpflichtung des Nutzers jede Änderung der Umstände mitzuteilen C9b) Im Falle von Organisationen, Überwachung von Benachrichtigungen über die Einstellung des Handels und Sperrung des Berechtigungsnachweises C9c) Vorgaben an Organisationen, dass die Registrierungsbehörde benachrichtigt werden muss, wenn der Berechtigungsnachweis, der an eine ihrer Angestellten für geschäftliche Zwecke ausgestellt wurde,

	gesperrt werden soll
R10) Nutzung des Berechtigungsnachweises für ungewollte Zwecke Ein Berechtigungsnachweis wird im Zusammenhang mit einer Transaktion benutzt, bei der der Aussteller wegen der Natur oder des Wertes der Transaktion nicht auf Garantieleistungen vorbereitet ist	Mögliche Maßnahmen, um das Risiko der Nutzung von Berechtigungsnachweisen für ungewollte Zwecke zu reduzieren, umfassen: C10a) Berechtigungsnachweise werden mit Anwendungsanweisungen ausgestellt C10b) Berechtigungsnachweise wie digitale Zertifikate, und die Tokens, die diese speichern, beinhalten Nutzungseinschränkungen C10c) An Stellen, an denen die Hauptgefahr für den Dienst von den Nutzern des Dienstes ausgeht, kann es nötig sein, die Identität eines Individuums näher am Punkt der Bereitstellung des Dienstes zu prüfen
R11) Entzug des Berechtigungsnachweises ohne bestimmten Grund Ein Berechtigungsnachweis wird aufgrund eines falschen oder bösartigen Berichts über eine Veränderung der Umstände oder eine Gefährdung des Berechtigungsnachweises entzogen	Mögliche Maßnahmen, um das Risiko eines, oder Unannehmlichkeiten durch, den unangemessenen Entzug des Berechtigungsnachweises zu reduzieren, umfassen: C11a) Fähigkeit den Berechtigungsnachweis auszusetzen und nicht sofort zu entziehen C11b) Ein Helpdesk Dienst, der dauerhaft für die Nutzer verfügbar ist C11c) Fähigkeit den Berechtigungsnachweis schnell nach Entzug zu ersetzen und/oder den Entzug zu widerrufen C11d) Registrierungsbehörden haben Zugang zu Verifikationsinformationen, um Garantien zu erhalten, dass die Person, die die Gefährdung oder die Änderung der Umstände berichtet, vertrauenswürdig ist
R12) Betrügerische Nutzung des Berechtigungsnachweises Ein Inhaber eines Berechtigungsnachweises versucht den Berechtigungsnachweis, entweder persönlich	Mögliche Maßnahmen, um das Risiko unbefugter Nutzung eines Berechtigungsnachweises zu reduzieren, umfassen: C12a) vertragliche Verpflichtung des Inhabers des

oder über Dritte für Transaktionen zu nutzen, für die dieser nicht berechtigt ist	Berechtigungsnachweises (Nutzer) diesen nur für seine vorgesehenen Zwecke zu verwenden C12b) Nutzung dynamischer Informationen, um zu überprüfen, dass der Berechtigungsnachweis noch vom richtigen Kunden gehalten wird C12c) Nutzung biometrischer Daten, um sicherzustellen, dass der Berechtigungsnachweis vom richtigen Kunden gehalten wird C12d) Vorgabe, dass die Nutzer sich vor der Verwendung für jeden Dienst registrieren und anmelden müssen C12e) Sicherstellung, dass Dienste in Übereinstimmung mit Einschränkungen der Nutzung des Berechtigungsnachweises bereitgestellt werden
R13) Hackerangriff Ein feindlicher Außenstehender erhält direkten Zugriff auf E-Government Dienstleistungen mit dem Ziel der Erreichung von persönlichen Vorteilen, Peinlichkeiten für das Vereinigte Königreich, Ablehnung des Zugangs zum System oder Verursachung von Schaden am System	Mögliche Maßnahmen, um das Risiko der Kompromittierung von Diensten aufgrund eines Hackerangriffs zu reduzieren, umfassen: C13a) Einsatz einer Firewall C13b) Eindringungstests C13c) Einsatz eines Intrusion Detection Systems (IDS) C13d) Pflege des Sicherheitszustandes der Geschäftsanwendungen und der Infrastruktursoftware
R14) Zerstreute Speicherung von Informationen Nutzerinformationen sind aufgrund der Verteilung von Daten, die durch verschiedene E-Government Dienstleistungen gesammelt wurden, einem größeren Kompromittierungsrisiko, ausgesetzt	Mögliche Maßnahmen, um das Kompromittierungsrisiko von Nutzerinformationen aufgrund von zerstreuter Speicherung zu reduzieren, umfassen: C14a) angemessenes Design der Dienste um die Vervielfältigung von Informationen zu minimieren C14b) Sicherstellung der Übereinstimmung mit dem Datenschutzgesetz

B. Internationale elektronische Ausweisprojekte

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
1	Access Card	Australien			http://www.efa.org.au/Issues/Privacy/accesscard.html		Die Pläne für die Access Card wurden 2007 von der Labor-Partei eingestellt.				abgelehnt	
2	ePassport	Belgien	ja but only the card holder's photo			19.11.2009	Since August 26, 2006 all passports are issued as a biometric passport with an embedded contactless smartcard RFID chip for storing biometric data			Introduced in 2004		
3	BELPIC eID card	Belgien	nein	eID, eGov, Esignature, Travel	http://eid.belgium.be/nl/FAQ/Over_de_eID/ http://eid.belgium.be/	03.12.2009	Belgium's 10 million citizens will use their new digital eID cards to file taxes, open bank accounts and make purchases on the Internet—through the card's unique ability to digitally authenticate identity.	mandatory for all citizens who has reached the age of 12. children between 6 and 12 years old are issued a kid's card.	keine	A foreigner card is issued to non-Belgiens with a residence permit of 5 years. Kost 10 Euro Kosten: 10-15€ Gültigkeit: 5 Jahre digitale Signatur: ja! Pflicht: ja!	eingeführt	2003
4		Dänemark								No national eID in Denmark under the notion of a national identification card		
5	Elektronischer Reisapass	Deutschland	ja		http://www.epass.de/	14.12.2009	Im November 2005 wurde in Deutschland der elektronische Reisepass (ePass) eingeführt. Er enthält das digitale Passfoto als erstes biometrisches Merkmal im Chip.					
6	Elektronischer Reiseausweis	Deutschland	ja		http://www.bmi.bund.de/cln_156/DE/Themen/Sicherheit/PaesseAusweise/eRei	17.12.2009	elektronischer Reiseausweis für Ausländer, für Flüchtlinge und für Staatenlose (eReiseausweis)				eingeführt	
7	Elektronischer Personalausweis	Deutschland	ja (2 Fingerabdrücke freiwillig, digital Foto ist verpflichtend)	eID, eGov, eSignature, Travel	http://www.bmi.bund.de/cln_156/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html	17.12.2009	Ab November 2010 wird der neue Personalausweis im Scheckkartenformat den bisherigen Personalausweis ablösen. Die neue Dokumentengeneration wird die herkömmlichen Anwendungen des Ausweises um elektronische Funktionen ergänzen. Die Daten, die heute optisch vom Dokument ablesbar sind, sollen zukünftig in einem Ausweis-Chip gespeichert werden. Damit können sich die Ausweisinhaber im Internet elektronisch ausweisen – sowohl gegenüber Behörden im E-Government als auch gegenüber privatwirtschaftlichen Dienstleistungsanbietern, beispielsweise bei Online-Shopping, Online-Banking oder beim Online-Kauf von Tickets. Gleichzeitig erhält der Ausweisinhaber über ein Zertifikat die Bestätigung, dass die von ihm	mandatory for citizens but online functionality, digital fingerprints and digital signatur are freiwillig	ICAO, CEN	Umsetzungsphase für den elektronischen Personalausweis beginnt. BMI gibt 30 Teilnehmer für den zentral koordinierten Anwendungstest bekannt.	geplant	
8	elektronischer Dienst- und Truppenausweis	Deutschland			http://www.bmi.bund.de/cln_156/DE/Themen/Sicherheit/PaesseAusweise/eDienstausweis/eDienstausweis_node.html	17.12.2009	Das Bundesministerium des Innern hat die Aufgabe übernommen, ein für die Bundesbehörden einheitliches Konzept für elektronische Dienst- und Truppenausweise aufzusetzen und die Ausweise dann zum Abruf bereit zu stellen.					

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
9	Gesundheitskarte	Deutschland	nein		http://www.bmg.bund.de/nn_1168300/DE/Gesundheit/Gesundheitskarte-Focuspage/gesundheitskarte__node.html	14.12.2009	Ziel ist eine praxisorientierte und sichere Telematikinfrastruktur, damit die Herausforderungen an ein technologisch hochentwickeltes und modernes Gesundheitswesen erfüllt werden können. Zunächst kommt eine erweiterte und datenschutzrechtlich sichere Krankenversichertenkarte mit Foto.	mandatory for citizens but the applications are freiwillig			geplant	
10	ESTeID eCard	Estland	nein	eID, eGov, eSignature, Travel	http://www.id.ee/10358	14.12.2009	The government of Estonia began distributing ID cards (personalised smartcards) to its citizens in January 2002. The cards contain the individual's name, address details, demographic information, as well as two PIN protected digital certificates and related cryptographic keys. A special distinction of this initiative is that Estonians can use their ID cards for accessing government services online and e-commerce applications, with both authentication and digital signatures being supported (by the separate certificates). The authentication certificate contains the individual's email address.	mandatory for citizens and permanent residents over the age of 15	keine	150 EEK	eingeführt	2003
11	FineID	Finnland	ja	eID, eGov, eBanking, eSignature, Travel	http://www.fineid.fi/vrk/fineid/home.nsf/pages/index_eng http://www.poliisi.fi/poliisi/home.nsf/pages/F082D8AB29097DB5C2256C29002BA66C?opendocument	03.12.2009		auf freiwilliger Basis an Bürger und Ausländer ab 6 Monaten Aufenthalt	keine	Kosten: Standard identity card EUR 48 Gültigkeit: 5 Jahre es gibt auch temporäre Karten für 4 Monate und 30 Euro Es ist möglich, sie als Krankenversicherungskarte zu benutzen elektronische Signatur: nicht bekannt	eingeführt	1999
12	PPI eID	Frankreich	ja	eID, eGov, eSignature, Travel	http://vosdroits.service-public.fr/particuliers/N360.xhtml	08.01.2009	Der elektronische Ausweis wird vom biometrischen Ausweis abgelöst, basierend auf der EG-Verordnung 2252/2004		ICAO, CEN	Kosten to be decided.	geplant	2010
13	ePassport	Griechenland	ja		http://www.passport.gov.gr/index.php?	14.12.2009						
14	Identity Card	Großbritannien	ja	eID, Travel	http://www.direct.gov.uk/en/Governmentcitizensandrights/Identitycards/index.htm	19.11.2009	As part of the National Identity Service, identity cards are being introduced alongside the UK passport. Both will include biometrics of your unique physical features (face and fingerprints), securing them to your biographic details (including your name, address, and date of birth). As the National Identity Service begins to roll out ID cards in 2009, residents in Greater Manchester will be able to enrol. In 2010, residents in northwest England will be able to sign up for a card as well. People who register their interest online now will be sent updates on the identity card programme as they occur. From 2012, every British citizen aged 16 or older will be able to apply for an identity card if they choose, but they	every British citizen aged 16 or older will be able to apply for an identity card if they choose, but they will not be required to have one	ICAO	Kosten: 30 Pfund	geplant/eingeführt	2009/2010

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
15	ePassport	Großbritanien			http://www.direct.gov.uk/en/TravelAndTransport/Passports/index.htm							
16	The italian Electronic Identity Card CIE (Carta d'Identita Elettronica)	Italien	ja	eID	http://www.esteri.it/MAE/EN/Ministero/Servizi/Stranieri/Sportello_Info/DomandeFrequenti/UfficiServiziConsolariEstero/Passaporti.htm http://www.innovations-report.de/html/berichte/informationstechnologie/bericht-26374.html	14.12.2009	The Italian Government system uses their National Services Card and Electronic ID card, both of which are smartcards, for citizen authentication with online government services. The Electronic ID card is a hybrid smartcard that also contains PIN protected personal data including the holder's blood group and fingerprint scans. A document that, as of 26 October 2006, has replaced former passports and is issued in Italy by the Italian Police (Questura) and abroad at Italian diplomatic-consular missions. It is valid for 10 years for all countries whose governments are recognised by the Italian government, except in the case of eventual legal limitations. It uses modern technologies that offer a high standard of security such an anti-fraud device and computer chip containing the data of its possessor and of the	verpflichtend an Bürger		25 Euro	eingeführt	2006
17	CNS	Italien	nein	eGov, eHealth, eSignature, eTicketing					keine	20 Euro	eingeführt	2006
	Reisepass	Liechtenstein	ja	ePass	http://www.liechtenstein.li/en/fl-aussenstelle-bern/fl-aussenstelle-bern-konsularisch/fl-aussenstelle-bern-konsularisch-reisedokumente.htm	08.01.2010	In dem PDF für den Antrag stehen einige Informationen: http://www.llv.li/pdf-llv-apa-wohnsitz-ch.pdf			10 Jahre gültig: CHF 130; 3 Jahre gültig: CHF 50	eingeführt	
	Reisepass	Luxembourg	ja	ePass	http://www.mae.lu/en/content/view/full/14237	08.01.2010	http://www.mae.lu/en/Site-MAE/Visas-Passports/Introduction-of-the-Biometric-Passport-fingerprints			5 Jahre gültig: 30€; 2 Jahre gültig: 20€	eingeführt	
18	DigiD	Niederlande			http://www.digid.nl/english/	19.11.2009	DigiD stands for Digital Identity and is a system shared between cooperating governmental agencies, allowing to digitally authenticate the identity of a person who applies for a transaction service via internet. With increasing numbers of public authority offices implementing the DigiD system, it is easy to begin using their range of electronic services after first choosing your own login code (user's name and password) at www.digid.nl. In short: DigiD provides users with a personalised login code for the full spectrum of contact with various governmental bodies. The Social Insurance Institute (SVB, Sociale Verzekeringsbank), the Centre for Work and Income (CWI, Centrum voor Werk en Inkomen), the Employees' Insurance and Benefits	Ausweispflicht seit 01.01.2005		offizielle Seite wenig aussagekräftig		
19	ePassport	Niederlande	ja		http://www.paspoortinformatie.nl/content.jsp?objectid=4495		A Dutch passport is issued to citizens of the Kingdom of the Netherlands (Dutch: Koninkrijk der Nederlanden) for the purpose of international travel. The passport also serves as a means of identification as required by the Dutch law since January 1, 2005 for all persons over the age of fourteen. Dutch passports are valid for a period of five years from issuing date. The passport complies to the rules (EG 2252/04) specified by the European Union. Since August 26, 2006 all passports are issued as a biometric passport with an embedded contactless smartcard RFID chip for storing biometric data.	required by the Dutch law since January 1, 2005 for all persons over the age of fourteen				

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
20	Bürgerkarte	Österreich	nein	eID, eGov, eHealth, eSignature	http://www.buergerkarte.at/de/index.html	19.11.2009	Die Bürgerkarte ist ein Schlüssel für die E-Government-Angebote der Verwaltung und für Web-Dienste der Wirtschaft. Diese Einsatzmöglichkeiten werden weiter ausgeweitet und die Bürgerkarte zum elektronischen Ausweis im Internet. Sie können die Bürgerkartenfunktion auf Ihrer e-card oder Ihrer Bankomatkarte aktivieren. Auch Studentenausweise oder Dienstausweise können zur Bürgerkarte gemacht werden. Hier finden Sie die dazu notwendigen Informationen.	Freiwillig an Bürger	keine	Kritischer Bericht zur Sicherheit http://www.heise.de/newsticker/meldung/Sicherheitsluecken-bei-oesterreichischer-Buergerkarte-trotz-Zertifizierung-219403.html Kosten: Für die e-card wird ein Service-Entgelt eingehoben, die Verwendung als Bürgerkarte	eingeführt	2004
21	e-card (Gesundheitskarte aber auch für e-Government Dienstleistungen)	Österreich			http://www.chipkarte.at/portal/index.html?ctrl:cmd=render&ctrl:window=ecardportal.start.startWindow&p_menuid=51682&p_tabid=1	17.12.2009	Mit der e-card Infrastruktur wurden die Schienen für eine Reihe zukunftsweisender Folgeprojekte gelegt. Die e-card ist für den Patienten mehr als nur ein Krankenschein in Scheckkartenformat. Sie ist der Schlüssel zum Gesundheitssystem und ermöglicht durch die Bürgerkartenfunktion auch den Zugang zu Services des E-Government.					
22	eID Card PLID	Polen	to be decided	eID, eGov, Travel	http://www.epractice.eu/en/document/288337				to be decided	Tests seit 14. April 2008 Einführung: bis 2013 für alle Pflicht: ja elektronische Signatur: ja	geplant	2010
23	Passaporte Electronico	Portugal	ja		http://www.pep.pt/vantagens_eng.html	14.12.2009						
24	The Portuguese eID Card Pegasus	Portugal	ja	eID, eGov, eTax, eHealth, eSignature, Travel	http://www.cartaodecidadao.pt/	14.12.2009	The citizen's card is a project that will contribute to make the modernisation of the Public Administration more dynamic. Cartão do Cidadão One aspect of the citizen's card is that in just one document it combines all the keys that are indispensable to a fast and effective relationship between the citizen and a variety of public services. The citizen's card is a technological development-friendly project. With its digital hat on, it will foster the development of electronic transactions by giving participants the peace of mind of a strong authentication and an electronic signature.		CEN	12 Euro		
25	Nationallet id kort (National eID)	Schweden	ja	eID, eGov, Esignature, Travel	http://www.polisen.se	14.12.2009			ICAO, CEN	Preis 400 SKR	eingeführt	2005
	Pass	Schweden	ja	ePass	http://www.rfidjournal.com/article/articleview/1942/1/1/	08.01.2009	Sweden has started issuing RFID-enabled passports, or e-passports, fitted with RFID tags. Each tag is encoded with the personal details normally included in a passport—height, hair and eye color, and so forth—and with a digital photograph of the owner.	Bürger	ISO 7816 and ISO 1443A standards. To prevent a tag from being read from a distance or by unauthorized personnel, each e-passport is printed with a basic access code (BAC). This code must first be read via an optical character recognition (OCR) scanner or typed in manually into the RFID interrogator, which compares the data in the BAC code with that in the RFID tag. If they match, the RFID interrogator will gain access to all information stored on the tag.			

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
26	Identitätskarte	Schweiz	ja		http://www.schweizerpass.admin.ch/pass/de/home/ausweise/identitaetskarte.html	14.12.2009		freiwillig an Bürger und Auslandsschweizer, verpflichtend für Ausländer mit Dauerwohnrecht		Weiterhin bleibt das familienfreundliche Kombiangebot (gleichzeitige Bestellung von Pass und Identitätskarte zum Spezialpreis von CHF 148.-- für Erwachsene und CHF 68.-- für Kinder) bestehen.		
27	E-Pass (PASS 10)	Schweiz	ja		http://www.schweizerpass.admin.ch/pass/de/home/ausweise/pass_10.html	17.12.2009	Pass 10 – der geplante E-Pass ab 2010 Als assoziierter Schengen-Staat ist die Schweiz verpflichtet, spätestens ab dem 1. März 2010 nur noch einen Pass mit elektronisch gespeichertem Gesichtsbild und zwei Fingerabdrücken auszustellen, einen so genannten E-Pass. Die bisherigen Schengen-Staaten mussten den E-Pass mit Gesichtsbild bereits per 28. August 2006 definitiv einführen. Ab 28. Juni 2009 müssen sie zusätzlich zwei elektronisch gespeicherte Fingerabdrücke in den Pässen speichern. Die definitive Einführung eines biometrischen Schweizer Passes stellt eine internationale Verpflichtung dar, deren Erfüllung weiterhin die Reisefreiheit der Schweizerinnen und Schweizer sicherstellen soll. Das Parlament hatte die Grundlagen für die definitive			Vorgeschlagene Preise des Bundesrats: Für Erwachsene 140 Franken, im Kombiangebot mit der ID 148 Franken, für Kinder- und Jugendliche 60 Franken bzw. 68 Franken im Kombiangebot. (140 Franken = ca. 92€) ob es einen Chip geben wird und ob elektronische	geplant	
28	PASS 06	Schweiz	ja		http://www.schweizerpass.admin.ch/pass/de/home/ausweise/pass_06.html	17.12.2009	Seit dem 4. September.2006 wird neben dem weiterhin aktuellen Pass 03 auch der Pass 06 ausgestellt. Dieser E-Pass unterscheidet sich äusserlich kaum vom Pass 03. Ein international anerkanntes Symbol für elektronisch lesbare Daten auf der Einband-Vorderseite kennzeichnet ihn. Zudem ist der Einband etwas dicker und härter als beim Pass 03. Grund: In ihm ist ein hauchdünner Chip untergebracht.					
29	eGK	Schweiz			http://www4.egk.ch/de/index.php		Elektornische Gesundheitskarte					
30	The Spanish eID Card DNIe	Spanien	ja	eID, eGov, Esignature, Travel	http://www.dnielectronico.es/Asi_es_el_dni_electronico/descripcion.html http://www.dnielectronico.es/Preguntas_Frecuentes/index.html	14.12.2009	Seit März 2006 Funktionen: • Digitale Unterschrift im Internet • Komplette Dienstwege online durchführen koennen • Sichere Transaktionen • Identifikation am Werkstor der Firma z.B. • Sicherheit am PC	verpflichtend an Bürger	keine	6,70 Euro	eingeführt	2006
31	National eID	Tschechien	nein	eID, eGov, Travel					CEN	Kosten: to be decided	geplant	2010
	Portal of the Public Administration	Tschechien	nein	eGov	http://portal.gov.cz/wps/portal/_s.155/19005	08.01.2010	Verschiedene Zertifikate: http://www.mvcr.cz/mvcren/scope-of-activities-egovernment.aspx		Certificates		eingeführt	

ID	Projekt Titel	Land	Biometrie	Funktionalitäten	Homepage des Projektes	Zugegriffen am	Kurze Projekt-beschreibung	Abgabe an wen	Standard	Kosten und Anmerkungen	Status	Einführungsdatum
32	STORK: Secure Identity Across Borders Linked	EU			http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=224993	19.11.2009	STORK eID - easier access to public services across the EU Several barriers to free movement of workers still exist in the EU: for example, it is not easy to access public services while working or living in another country. The European Commission has launched a pilot project to remedy this situation with an EU-wide system for the recognition and authentication of electronic identity (eID via electronic cards or other means). It will enable businesses and citizens to securely use their national electronic identities and get help from public administrations in any Member State they live in or travel to.					
33	European Citizen Card, ECC	Europäische Union								http://www.kes.info/archiv/online/07-2-010.htm		
34	Führerschein, Sozial- versicherungs-ausweis	USA			http://www.govtrack.us/congress/billtext.xpd?bill=h109-418		In den USA gibt es nichts dem Personalausweis vergleichbares. Meist wird der Führerschein als Ausweis benutzt oder die Sozialversicherungsnummer. Der REAL ID Act möchte den Führerschein zum allgemeinen Ausweis machen.					
35	Reisepass	USA			http://travel.state.gov/passport/ppt_card/ppt_card_3926.html		Reisepässe besitzen nur 20% der Amerikaner, wurden aber jetzt auf Scheckkarten-Format mit RFID umgestellt. Kosten: 45$ Gültigkeit: 10 Jahre (für unter 16 jährige: 5 Jahre) Basis: freiwillig Start: 14. Juli 2008 Anscheinend keine digitale Signatur					
36	Reisepass	weltweit	ja	ePass	http://www2.icao.int/en/MRTD/Pages/default.aspx	08.01.2010	A Machine Readable Travel Document (MRTD) is an international travel document (e.g. a passport or visa) containing eye-and machine-readable data. Each type of MRTD contains, in a standard format, the holder's identification details, including a photograph or digital image, with mandatory identity elements reflected in a two-line machine readable zone (MRZ) printed in Optical Character Recognition-B (OCR-B) style. Standardization of elements in the travel document allows all participating countries inter-operability. This "global inter-operability" of MRTDs facilitates inspection of international travellers at borders and generally enhances security.	Reisepass --> Flugreisende	Machine Readable Travel Document (MRTD)		As of 1 August 2009, over 170 States had issued MRPs that comply with the ICAO standard, and by 1 April 2010 all Contracting States must do so.	2010
37	Reisepass	Europäische Union	ja	ePass	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:DE:HTML	08.01.2020	Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten	EU-Bürger		länderspezifisch		Fingerabdrücke: bis 29.06.2009; Gesichtsbilder bis: 28.08.2006

C. Bedenken von Bürgern

In der unteren Tabelle sind die Hauptkritikpunkte von digitalen Ausweisprojekten in Deutschland zusammengefasst. Da es sich bei allen um Zitate handelt, haben wir zur leichteren Lesbarkeit die Anführungszeichen weggelassen.

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Wir sind doch eh schon gläserne Menschen und wer das nicht zur Kenntnis nehmen will, der hat den Knall immer noch nicht gehört. Die Aussagen in "Orwell 84" waren ja nur ein Abklatsch dessen, was inzwischen zu Lasten von Freiheit und Menschenrechten, nicht nur im GG sondern in der Realität von diesem Rollifahrer verändert wurde.	12.05.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	negativ
Vertrauen	Mit der Einführung des Euro hieß es "er sei fälschungssicher". Mit der Einführung der Bankgeschäft via Internet hieß es "es sei sicher", mit der Einführung der eCard im Gesundheitswesen heißt es "sie sei sicher" ... Es ist nur eines sicher: Nichts ist sicher!	09.03.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	negativ
Vertrauen	Im Ausland hat man das schon lange, z. B. Spanien. Hier ist es für mich schon wieder eine Kostenfrage: Was muss der Bürger berappen?. Des weiteren sehe ich nach Stasi, mehreren Abhör- u. Überwachungsskandälen, wie Lidl, Telekom u. Bahn, die ich merkwürdiger Weise nicht für die einzigen halte, die uns ausdauernd bespitzeln, auch die Gefahr noch mehr zu einer gläsernen Person zu werden. Denn wer kann schon ermessen, was für Daten gespeichert sind? Es sind doch die wenigsten. Eigentlich geht es in der Krankenkasse los. Was ist wirklich auf meiner Chipkarte?	15.02.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	negativ
Vertrauen	Ich denke, dass es NICHT notwendig ist, einen neuen PA einzuführen. Einzig aus Gründen der Überwachung und des "gläsern" machens der Bürger dieses Landes. Heute ein neuer PA mit Chip und morgen ein Chip mit GPS im Körper implantiert. In den USA wird damit schon seit Jahren rumexperimentiert. Was das bringen soll liegt klar auf der Hand. Per Chip ist man leicht zu orten, per Chip ist es möglich alle persönlichen Daten über eine Person abzufragen und wenn nötig kann man die natürlich auch dazu einsetzen, diese Person völlig abzutrennen von allem, was ihn beweglich und flexibel macht, wie z.Bsp. Bankkonten. Ohne Geld, geht so gut wie gar nichts mehr. Wir haben uns mit der heutigen Technologie und dem Geld so abhängig gemacht, dass wir hilflos wären ohne Technik und Kreditkarte. Man wird an Orwell erinnert, den totalen Überwachungsstaat und an Filme aus Hollywood wie "Staatsfeind Nr. 1" u. ä. Ich kann nur davor warnen! Es ist ein Angriff auf die Mündigkeit der Bürger. Wieder ein Schritt in Richtung Versklavung der Menschen durch das Kapital. Und zahlen müssen wir natürlich auch noch dafür SELBST.	14.02.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Das ist cool. Es werden Vertragsabschlüsse online erleichtert, geschäftliche Abwicklungen, Anfragen bei Behörden u.v.m. . Eine Kopie des Personalausweises wird kaum noch erforderlich sein. Ich werde auf einen Fingerabdruck nicht verzichten. Denn sollte der Ausweis abhanden kommen , könnte man nichts damit anfangen.	14.02.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	positiv
Vertrauen	Ein weiterer Schritt in Richtung der totalen Überwachung. Orwell läßt grüßen.	14.02.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	negativ
Vertrauen	Solange wie ich dafür nicht meine Fingerabdrücke abliefern muss, is mir das egal.	14.02.2009	http://www.webnews.de/kommentare/333292/0/Der-E-Ausweis-kommt.html	Der E-Ausweis kommt	
Vertrauen	Ein elektronischer Personalausweis – mit oder ohne Pseudonymfunktion – hat aus meiner Sicht eigentlich nur Nachteile, ausser dem offensichtlichen Vorteil, nur noch eine Karte im Portemonnaie herumtragen zu muessen. Der Hauptnachteil ist natuerlich, dass viele Anbieter aus Kostengruenden auf ein eigenes ID-System verzichten koennten und der ePA zu einem zwangsweisen single-sign-on wird. Wenn Karte und PIN abhanden kommt, stehen also alle Tueren offen.	15.02.2009	http://www.datenschutzbeauftragter-online.de/e-personalausweis-soll-pseudonym-funktion-erhalten/	E-Personalausweis soll Pseudonym-Funktion erhalten	negativ
Sicherheit	das ist nur geldmacherei der politiker. mit der heutigen technik kann man alles fälschen. ich gebe ein bis zwei jahre nach einführung des e-ausweises, dann tauchen die ersten falschen auf. wenn es überhaupt solange dau…	15.02.2009	http://www.bild.de/BILD/politik/2009/02/13/personalausweis/bundesrat-macht-weg-fuer-elektronischen-personalausweis-frei.html	Einführung beschlossen Der E-Ausweis kommt	negativ
Vertrauen	Nachdem unser Staat ja auch keine Onlinedurchsuchungen veranlasst, wie man ja anhand diverser Fälle der Vergangenheit sehen kann, glaube ich den Politikern natürlich das meine Fingerabdrücke nur auf dem Perso und nicht in einer Zentraldatei gespeichert werden... nee is klar! Die Stasi war ein Witz im vergleich zu Schäuble&Co.	22.04.2008	http://www.welt.de/politik/article1924422/Gehoeren_Fingerabdruecke_in_den_Ausweis.html	Elektronischer Pass Gehören Fingerabdrücke in den Ausweis?	negativ
Vertrauen	Schäuble & Co. scheinen mir extrem gefährlich mit ihrem Ansinnen auf Sicherheit und weiteren blödsinigen Argumenten. Tatsache ist, dass derartige Unterfangen auf einen einen Überwachungsstaat hinauslaufen.	23.04.2008	http://www.welt.de/politik/article1924422/Gehoeren_Fingerabdruecke_in_den_Ausweis.html	Elektronischer Pass Gehören Fingerabdrücke in den Ausweis?	negativ
Vertrauen	Wer nichts zu verbergen hat, der kann all diese Sachen angeben. Was soll denn damit passieren? Wird schon keiner geklont werden. Wenn es der Sicherheit und der Einfachheit dient, bin ich damit zu 100% einverstanden. Diese ständige übertriebene DAtenschützerei ietet Kriminellen zusehens rechtsfreie Räume!	11.09.2008	http://www.welt.de/politik/article1924422/Gehoeren_Fingerabdruecke_in_den_Ausweis.html	Elektronischer Pass Gehören Fingerabdrücke in den Ausweis?	positiv

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Merkwürdig dabei ist doch, dass Diplomaten-Pässe von diesen (F)Unkchips verschont bleiben. Das ist der Bundesregierung dann nämlich doch zu unsicher. Die Problemlosigkeit mit der dieser Chip aus 1m Entfernung geklont werden kann, ist frappierend und beschämend für unsere Innenminister. Die Fingerabdruckabgabe für Unbescholtene könnte ebensogut eine Idee der Nazis sein. Der Sicherheitswahn führt zu missbrauch totalitären Systemen. Das beste Beispiel dafür war die DDR mit dem MfS (Stasi). Wir bewegen uns zurück. Hoffendlich nicht zu weit.	01.11.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Alle sprechen von dem E-Pass, aber wie werden bei einer Kontrolle die Fingerabdrücke gesichert? Hier gibt es ein erneutes Sicherheitsproblem.	01.11.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Wenn man schon wieder vor Beginn des Ganzen behauptet, der Datenschutz sei 100prozentig und die Systeme wären nicht zu knacken. Bisher war jedes System zu knacken und auch dieses wird es sein. Was das ganze nur noch schlimmer macht, denn wenn dann ein gefälschter Pass benutzt wird, wird es noch nicht einmal auffallen bzw. es wird nahezu unmöglich, ihn zu finden.	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Wie war man damals bei der Volkszählung noch datenbewusst. Inzwischen geht es ja richtig ab in Richtung Überwachungsstaat. Es scheint keine Hemmungen mehr zu geben, das technisch Mögliche auch zu realisieren. Es ist ja nicht nur ein einzelner Aspekt. Eine Unzahl von Kameras allerorten (fast keine gekennzeichnet). Die Versichertenkarte der Krankenversicherung enthält persönliches Material usw...	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Die Einführung von neuen Reisepässen ist eine sinnvolle Maßnahme, um zahlreiche Probleme besser bekämpfen zu können! Wir leben in einer globalisierten Welt mit offenen Grenzen in Europa. Diese neue Dimension der Freiheit eröffnet große Chancen, sie bringt aber auch Probleme mit sich. Die organisierte Kriminalität profitiert besonders von den offenen Grenzen. Egal ob es um Drogen, Waffen, Schmuggelware oder sogar Menschenhandel und Kinderpornographie geht: Diesen neuen Reisepässe garantieren eine bessere Überprüfung der jeweiligen Person! So lange der Datenschutz eingehalten wird sehe ich keinen Grund für Bedenken. Man sollte auch nicht übersehen, dass die Folgen der organisierten Kriminalität für viele Menschen gravierend sind, zudem ist der finanzielle Schaden enorm und nicht hinnehmbar!	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	positiv
Vertrauen	die ohne Wissen des Passinhabers von dem in der Warteschlange an der Supermarktkasse etc. hinter ihm Stehenden bedient, die Passdaten auslesen. Zugriffscodes für EAC verbreiten sich über undichte Stellen bei Herstellern und Behörden-insbesondere im Ausland-in der kriminellen Szene und übers Internet. Der Weg zur Massenkompromittierung und dem gläsernen Bewohner wird freier.	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Ein weiterer Überwachungsschritt Richtung "Neue Weltordnung". Fingerabdrücke und der RFID-Chip, wie er auch inzwischen von Karstadt und Kaufhof eingesetzt wird, sind weitere Schritte zu Bürgerüberwachung. Damit das akzeptiert wird braucht man den "Terror". Der Chip unter der Haut ist eins der Endziele. Dieser kann nicht nur senden sondern auch empfangen.	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Orwell laesst gruessen und der dt. Staat ist wie immer der Vorreiter. Ich warte auf die 3. Stufe und dann die Kuer, die Einpflanzung von RFD-Chips bei Neugeborenen! Deutschland Ueberwachungsland! Besser Deutschland ade.	30.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Vertrauen	Wie kann man diesen orwellschen Unfug eigentlich lahm legen? Einen großen Magneten ranhalten? Oder im Kaufhaus mal auf die Löschplatte vom Diebstahlschutz legen? Warum bekommen wir nicht gleich einen Chip unter die Haut, wie Hunde?	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
	Nicht koscher! Schily war direkt an die Auftragsvergabe an Biometrie Firmen beteiligt, in dessen Aufsichtsratmitglied er heute sitzt.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
	Bürgerfinanzierter Millionenauftrag! 2006 hat Otto Schily schon Stammaktien bei einer dieser Firmen erworben.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Datenschutz	Wer hat nichts zu verbergen "Ich habe nichts zu verbergen" ist die dümmste und damit gefährlichste Aussage in der Diskussion um den Überwachungsstaat. Ein Gendefekt geht z. B. keinen Arbeitgeber etwas an. Dass jemand zufällig im gleichen Zug wie ein Attentäter saß, geht niemanden etwas an. Man könnte daraus nämlich vorsorglich Maßnahmen ableiten. Werden Informationen gesammelt, so werden sie auch irgendwann genutzt.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
	Das ist eine Rießensauerei! Otto Schily hat doch sein Amtszeit ausgenutzt um diese Pässe einzuführen, und heute sahnt er als Aufsichtsratsvorsitzender kräftig ab.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Datenschutz	Gut so! Endlich mal etwas sinnvolles! Vor allem da die Daten ja nur im Pass und nicht zentral gespeichert werden. Ich habe nichts zu verbergen und somit auch nichts dagegen wenn von mir Fingerabdrücke genommen werden.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	positiv
Sicherheit	Nichts Neues In vielen Ländern Europas gibt es den Fingerabdruck im Pass schon seit den 80er Jahren, z.B. in Spanien. Nun sind Dokumente relativ sicher einer Person zuzuordnen, vorher war dies mitnichten der Fall. Gleiches müsste im Prinzip auch mit den Krankenversicherungskärtchen geschehen, da diese beliebig herumreichbar sind.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	positiv

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Sicherheit	Mit Fingerabdruck ist gut So kommt es zu keiner Verwechslung mit gesuchten Personen.Mir ist ein Fall bekannt,der fast zu einer Verhaftung führte, weil Name und Geburtsdatum des Passinhabers mit einer gesuchten Person identisch waren.Im Allgemeinen wird sich bei Passkontrollen nichts ändern.Sie werden weiterhin, zumindest in Europa, zügig und reibungslos verlaufen und nur auf Verdacht wird man den Fingerabdruck überprüfen.	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	positiv
Vertrauen	Orwell Die Totale Kontrolle der Bevölkerung ist nicht läger die Erzählung eines George Orwell "1984". Es wird zur Realität und jeder sieht dabei zu, wo bleibt die Kritik der Medien...Pressefreiheit bedeutet nicht, wichtige Informationen wegzulassen!!!!	29.10.2007	http://www.focus.de/digital/multimedia/tid-7582/e-pass_aid_134930.html	E-Pass Ausweis speichert Fingerabdrücke	negativ
Sicherheit	naja, warum überhaupt Fingerabdrücke aufnehmen lassen? Warum nicht Sekundenkleber auf die Kuppen und bei der Paßbeantragung halt unschuldig schauen und mit den Achseln zucken. Manche Berufe (handwerklich z.B. oder Laborberufe) haben eben das Risiko, dass die Fingerkuppen keine/nicht interpretierbare Muster aufweisen. Klappt auch in D.	07.12.2009	http://www.netzpolitik.org/2009/fingerabdruecke-fuer-einreise-chirurgisch-veraendert/#comments	Fingerabdrücke für Einreise chirurgisch verändert	negativ
Vertrauen	Heute ist ja mal wieder ein wahrer Freiheitstag. Ueberwachungs-Bullshit-Bingo vom Feinsten.	17.12.2008	http://www.netzpolitik.org/2008/innenausschuss-macht-weg-frei-fuer-neue-personalausweise/#comments	Innenausschuss macht Weg frei für neue Personalausweise	negativ
Sicherheit	[quote]Ausweise würden ihren Inhabern gezielt gestohlen und dann von fremden Personen verwendet, die den Inhabern ähnlich sehen oder sich ein ähnliches Aussehen durch Änderung von Frisur oder Brille verschaffen würden. Bei biometrischen Kontrollen sei dieser Missbrauch nicht mehr möglich, hofft die Regierung.[/quote] Nunja, und was soll dann ein Bürger machen, der sein Aussehen aus persönlichen oder ästhetischen Gründen ändern möchte und sich eine neue Frisur schneiden lässt? Wird der dann pauschal bei der vollautomatisierten Kontrolle am Flughafen ausgesperrt? Denn man kann nicht beides haben: Entweder man möchte verhindern, dass sich ähnlich sehende Menschen ihre Identitäten austauschen können oder aber man lässt den Bürgern ihre Freiheit, ab und zu ihr Aussehen zu ändern.	15.12.2008	http://www.netzpolitik.org/2008/gesetzentwurf-zu-elektronischem-personalausweis-und-elektronischer-identifizierung/#comments	Gesetzentwurf zu elektronischem Personalausweis und elektronischer Identifizierung	negativ
Sicherheit	Die Fingerabdrücke sind freiwillig. Außerdem steht im Gesetzentwurf drin, dass der Fingerabdruck unterbleibt, wenn aus medizinischen oder körperlichen Gründen keine verwertbaren Fingerabdrücke genommen werden können.	15.12.2008	http://www.netzpolitik.org/2008/gesetzentwurf-zu-elektronischem-personalausweis-und-elektronischer-identifizierung/#comments	Gesetzentwurf zu elektronischem Personalausweis und elektronischer Identifizierung	positiv

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	es ist leider traurige tatsache, dass die informationspolitik der regierung zu wünschen übrig läßt. ich glaube kaum, dass sich daran viel ändern wird in nächster zeit.	15.09.2008	http://www.netzpolitik.org/2008/epass-die-werden-jeden-quatsch-unterschreiben/#comments	ePass: Die werden jeden Quatsch unterschreiben	negativ
Vertrauen	Superschnell vorauseilend haben unsere Politfuzzis den EU-Wunsch nach dem Fingerabdruckpass erfüllt. Wären sie nur einmal so schnell bei der Umsetzung von EU-Beschlüssen, die dem Bürger zustatten kommen sollen, hier verstreichen die Fristsetzungen aber immer wieder ohne Resultate. Oder, Moment mal, was haben die Lobbyisten der RFID-Chip Produzenten gespendet, um sich an ihren Schnüffelchips, gesetzlich? dem Wähler in den Pass gezwungen, eine goldene Nase zu verdienen?	02.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ
Vertrauen	Fingerabdrücke - W A R U M ???????? Hier geht es NICHT um evtl. mehr Sicherheit - sondern um Umsatz für die Sicherheits- und Passdrucker, und zwar europaweit! Für die (privatisierte) Bundesdruckerei war der EU-Beschluss Rettung vor der Pleite in letzter Sekunde. Aber auch die Wettbewerber wie G+D, Oberthur, De La Rue, Crane/Setc, Tumba Bruk etc, liessen die Sektkorken knallen, als die EU beschloss, Fingerabdrücke in Pässe zu speichern. Ein gigantischer Umsatz-Jackpot, der seinesgleichen sucht, wurde hier verteilt!! Hinzu kommt die gewaltige Peripheri wie Passleser, Fingerprint-Scanner, neue Software, laufende (kostspielige) Up-Dates, Umbauten an Flughäfen und Grenzkontrollstellen, neue Netzwerke etc. etc. Es wäre nicht verwunderlich, wenn die Sicherheitsbranche Osama Bin Laden ein Denkmal setzt.	01.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ
Sicherheit	Tja, wie nun...??? Tja, jetzt muss nur noch eine Gesetzesinitiative her, die Ausländische Attentäter / Terroristen dazu verpflichtet, vor der Einreise einen deutschen Reisepass zu beantragen. Wär ja noch schöner, wenn die unsere Sicherheitsinitative umgehen, indem sie einfach mit einem Reisepass aus ihrem Heimatland einreisen...	01.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ
Vertrauen	Big Brother ist watchin your - Orwells utopische Phantasien sind längst Realität! Das Schlimme aber ist, es regt sich schon kaum einer mehr darüber auf, man stumpft offensichtlich langsam ab gegenüber den vielen (subtilen) Überwachungsmechanismen.	01.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Wieder ein Schritt näher.... ...an der übersichtlichen Speicherung der personenbezogenen Daten eines ganzen Volkes. Diese Verlogenheit und Verharmlosung geht mir gewaltig auf den Zeiger. Datenschützer waren davor, werden aber von den Verantwortlichen nicht mehr ernst genommen. Und was machen wir dann wieder, wir akzeptieren es. In vernetzten Systemen ist die Weitergabe von Daten der Bürger dann ein Einfaches. Und ein BKA freut sich schon jetzt darauf, Fingerabdrücke aller Bürger abspeichern zu können. Das muss ja nicht offiziell passieren. Mir soll mal einer beweisen, daß es so nicht ist. Den Verantwortlichen glaube ich keine Silbe mehr ! Die Fakten wie von chris_le beschrieben, zeigen es doch auf !	01.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ
Vertrauen	Mein Reisepass landet erst mal in der Mikrowelle oder ich werde einen Reisepass ohne Fingerabdrücke beantragen. dann stelle ich halt ein Visum, wenn ich unbedingt in dieses Land muss. Und diese Ausweise sollen fälschungssicher sein. Ich lache mich tod.	01.11.2007	http://www.stern.de/wissen/technik/der-neue-e-pass-fingerabdruecke-gehen-auf-reisen-601440.html	Der neue E-Pass: Fingerabdrücke gehen auf Reisen	negativ
Sicherheit	Angeblich nur ein paar cm. Es hat aber Versuche gegeben bei denen weit über 100m geschaft wurden. Hier wird auch der Sinn und zweck des neuen Passes deutlich.	17.11.2005	http://www.heise.de/ct/artikel/Die-Auseinandersetzung-um-Ausweise-mit-digitalisierten-biometrischen-Merkmalen-302400.html	Die Auseinandersetzung um Ausweise mit digitalisierten biometrischen Merkmalen	negativ
Vertrauen	Es geht um eine Möglichkeit Bewegungsprofile zu erhalten. Wenn man ein Gebäude mit genügend Sensoren ausstattet kann man cm-Genau sagen wo sich jemand aufhält. Alle anderen Argumente halte ich für absoluten Käse. Es wird mit Sicherheit nicht ein einziger Anschlag durch diese Pässe verhindert (die "richtigen" Terroristen haben halt ganz einfach einen gültigen echten Pass). Was schwindet sind die Grundrechte der normalen Bürger. Das Ende ist eindeutig eine Diktatur. Augen auf... bevor es zu spät ist....	17.11.2005	http://www.heise.de/ct/artikel/Die-Auseinandersetzung-um-Ausweise-mit-digitalisierten-biometrischen-Merkmalen-302400.html	Die Auseinandersetzung um Ausweise mit digitalisierten biometrischen Merkmalen	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	>Die Terminvorgabe der USA, nach der Staaten bis zum Oktober 2004 biometrische >Merkmale in ihren Pässen einbinden sollen, erklärte Hamann für unrealistisch. Finde ich gut, dass er das gesagt hat. Das einzige was mit den biometrischen Merkmalen im Verbund mit rfid leichter wird, ist die Kontrolle des Staates über seine Bürger. Terroristen werden leider immer Mittel und Wege finden dies zu umgehen. Somit ist es für den Normalbürger nur eine Pseudosicherheit und für den Staat ein zusätzliches Überwachungsfeature.	19.03.2004	http://www.heise.de/newsticker/meldung/Reisepass-mit-RFID-Chip-95597.html	Reisepass mit RFID-Chip read-only	negativ
Vertrauen	Alles halb so schlimm ich weisz das klingt provokant. aber folgendes szenario. in berlin rennt die polizei immernoch mit funkgeraeten von 1970-1975(!) herum. ergo: die taugen nix und sind analog-unverschluesselt. die bekommen aber keine neuen, weil weder kohle da ist, noch die innenminister sich auf standards einigen koennen. d.h. wenn ein ordnungshueter in B an der S in einen Keller geht um verdaechtige zu verfolgen, benutzt er fuer den Kontakt mit der Zentrale was? richtig. sein PRIVATES mobiltelefon. auf EIGENE rechnung. d.h. wir sollten hoffen, dasz vater staat so bankrott bleibt, wie er ist, dann wird's niemals hinreichend viele rfid-scanner geben, dasz es sinnvoll waere, rfid-paessei einzufuehren.	19.03.2004	http://www.heise.de/newsticker/meldung/Reisepass-mit-RFID-Chip-95597.html	Reisepass mit RFID-Chip read-only	positiv
Vertrauen	Was bringt der RFID-Chip das ein maschinenlesbarer Pass nicht bringt? Der einzige Unterschied den ich erkennen kann ist dass man dann nicht mehr notwendigerweise merkt ob der Pass geprueft wird. Der Sicherheitsgewinn davon ist was?	19.03.2004	http://www.heise.de/newsticker/meldung/Reisepass-mit-RFID-Chip-95597.html	Reisepass mit RFID-Chip read-only	negativ
Sicherheit	Ich wette, dass diese Technik es den Profis leichter machen wird. Wenn sich die Personenkontrolle vom Auge-zu-Auge-Prinzip verabschiedet und man sich dann völlig auf die maschinelle Verifikation verläßt, dann haben's die Profifälscher leicht. Denn die RFID-Chip-Pas-Entwickler können mir nicht erzählen, dass man diese Chips nicht nachbauen/verändern/umprogrammieren kann. Ich ahne schlimmes.	19.03.2004	http://www.heise.de/newsticker/meldung/Reisepass-mit-RFID-Chip-95597.html	Reisepass mit RFID-Chip read-only	negativ
Vertrauen	Wie robust sind diese RFID-Chips eigentlich? Gesetzt den Fall, ich lege ein Handtuch auf einen solchen Reisepass und bearbeite ihn dann vorsichtig mit der Breitseite eines Hammers. Überlebt er das?	19.03.2004	http://www.heise.de/newsticker/meldung/Reisepass-mit-RFID-Chip-95597.html	Reisepass mit RFID-Chip read-only	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Und wie schon beim ePass werde ich bis kurz vor Toresschluss warten, um mir dann noch den alten zu holen. Warte jetzt schon über 1 Jahr mit 'nem abgelaufenen Ausweis. Aber da ich ja 'nen gültigen Pass habe, kostet das ja keine Strafe. Einzig um die Frage des Biometriefotos muß ich mich noch "kümmern", denn das muß man ja schon abgeben, wenn ich das recht erinnere.	25.09.2008	http://blog.kairaven.de/archives/1650-Chaosradio-sendet-zum-elektronischen-Personalausweis.html	Chaosradio sendet zum elektronischen Personalausweis	negativ
Sicherheit	AW: Elektronischer Personalausweis kommt am 1. November 2010 Ist bereits geknackt... Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender adam laurie hat 12 min. dafür gebraucht... hat noch gleich einen Clone erstellt. Ein neuer Reisepass ohne Fingerabdruck ist gar nicht mehr möglich nach meinen Informationen. Wer nicht mehr ins Schema passt, dem wird ein Fingerabdruck am Verbrechensort/i.Zukunft ein Computer-Hack unter geschoben...	19.12.2009	http://www.pcgameshardware.de/aid,701443/Elektronischer-Personalausweis-kommt-am-1-November-2010/Technologie/News/	Elektronischer Personalausweis kommt am 1. November 2010	negativ
Vertrauen	Schöne neue Zeit... Musste der METRO Konzern nicht vor ein paar Jahren etliche Kundenkarten tauschen, wegen RFID-Chips? Die wollten doch damit Bewegungsprofile aufzeichnen um die Waren noch besser präsentieren zu können, etc. Dann könnte mit Hilfe des neuen Personalausweises das ganze doch auch problemlos funktionieren. Dann würde endlich diese lästige Software mit dem Facetracking der öffentlichen Kameras noch viel besser funktionieren... Und bei viel weniger Aufwand... Und ja, auf jeden Fall würde ich mit meinen "Perso-Daten" im Internet shoppen gehen, meine Kreditkarte benutze ich ja auch nur OHNE SSL Verbindung... Oder ist das nicht sicher? Man bekommt doch ´ne neue wenn das Konto leer ist, oder? Der gläserne Mensch wird immer mehr zur Realität und was uns da alles noch passieren kann, würde gerne mal 50 Jahre in die Zukunft schauen...	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ
Vertrauen	Der CCC hat da ne Anleitung für nen EMP zum selberbasteln. Der überlädt jeden RFID-Chip zuverlässig ohne äußerliche Spuren..	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Mein neuer Perso wird wohl erstmal eine Runde Karussell in der Mikro fahren. Dann brauch ich mir auch keine Gedanken mehr über RFID und Co machen. Hätte man nicht statt dem Akronym RFID das sich jedesmal wenn man es ausspricht nach einer schweren Erkältung anhört ein Backronym nehmen können das mann aussprechen kann? Vielleicht ROC, Radio Observing Chip oder irgendetwas anderes das man aussprechen kann.	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ
Vertrauen	Wie groß ist die Reichweite dieser chips? Könnte man den Chip aus größerer Distanz als wenigen mm lesen würde ich es für bedenklich halten. Dann könnte man mich auf meinem Weg zum, durch und zurück vom Supermarkt(z.B) verfolgen. Unangenehmer Gedanke. Muss ich ihn allerdings wirklich SEHR nah an ein Lesegerät halten könnten durchaus die vielen Vorteile überwiegen.	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	positiv
Vertrauen	einfach den alten perso behalten und sich gegen den neuen wehren! keiner ist verpflichtet sich ausweisen zu könne (allg. irrglaube, ihr seid deutsche staatsbrüger mit eurem namen kann die polizei genug anfangen, die daten mit bild sind hinterlegt)! ... ich werd die nächsten 30 jahre mit nem abgelaufenen perso rumlaufen, na und?	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ
Sicherheit	Es gibt mittlerweile doch schon RFID sichere Hüllen. Ansonsten tut es auch die gute alte Alufolie und wenn das nicht reicht kann man sich daraus auch einen Hut basteln gegen Gedankenkontrolle und Stasi 2.0 Bespitzelung.	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ
Sicherheit	Nicht jeder RFID chip hat die Reichweite. Es ist abhänging von der geplanten Anwendung. Man kann RFID auch für Reichweiten von 10cm nutzen/auslegen.	16.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	positiv
Vertrauen	Auch 10cm sind zu viel! Dann brauch ja ein Lesegrät nur heimlich jemandem an die Gesäßtasche halten und ich weiß wer er ist. Nein danke, dass muss nicht sein. mehr als direkter Kontakt (bzw. wenige mm) wäre zuviel. Ansonsten halte ich das ganze für keine schlechte idee, da es ja doch auch einige Vorteile gibt	17.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	positiv
Vertrauen	Finde ich wirklich gut das die EU nun immer "hacker-freundlicher" wird, da freut man sich doch wenn man endlich mal Konten unter anderem Namen ohne Probleme anlegen kann ohne aufwendig einen Ausweis zu fälschen. Weiter so!	18.12.2009	http://www.tomshardware.com/de/Elektronischer-Personalausweis-RFID-Fingerabdruck,news-243839.html	Elektronischer Personalausweis: Scheckkartenformat und RFID-Sender	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Sicherheit	Der Datenmissbrauch findet doch nicht bei den Bürgern statt (die kontrolliert werden sollen) sondern in der Industrie, die hier (bewusst) massenweise Datengeschacher betreibt. Da helfen auch alle Personalausweise, Gesundheitskarten und De-Mails nichts.	08.12.2009	http://www.welt.de/webwelt/article5464940/Durchwachsende-Bilanz-auf-dem-IT-Gipfel.html	Informationstechnik Durchwachsende Bilanz auf dem IT-Gipfel	negativ
Vertrauen	Ich habe auch keine Angst um die Sicherheit meiner Daten und die Integrität meines PCs und muss daher nicht vom Staat ständig am Gängelband gehalten werden (wie die 87% der (D)ümmsten (A)nzunehmender (U)ser von denen unser Innenminister berichtet).	08.12.2009	http://www.welt.de/webwelt/article5464940/Durchwachsende-Bilanz-auf-dem-IT-Gipfel.html	Informationstechnik Durchwachsende Bilanz auf dem IT-Gipfel	positiv
Vertrauen	Da bin ich skeptisch Zahlungsverkehrsdaten zur freien Verfügung, absolut unkontrolliert an die USA auszuliefern, Datenpannen bei staatsnahen Institutionen und bei Privatunternehmen nahezu täglich. Erst mal das eigene...	08.12.2009	http://www.bbv-net.de/public/article/digitale/792926/Politik-fordert-mehr-Sicherheit-im-Netz.html	IT-Gipfel in Stuttgart Politik fordert mehr Sicherheit im Netz	negativ
Sicherheit	Sicher sollte Kriminalität etc. nicht Tür und Tor geöffnet werden aber irgendwie sollte man doch auch auf dem Boden bleiben. Hier geht es unserer Politik, egal wem, egal in welchem Bereich nur um eins, uns Menschen extrem kontrollieren und bevormunden zu können, um sonst nichts. Mich würde es noch nicht mal wundern, wenn man sich in Zukunft für einen Gang zur Toilette auch noch an und abmelden muß.	08.12.2009	http://www.bbv-net.de/public/article/digitale/792926/Politik-fordert-mehr-Sicherheit-im-Netz.html	IT-Gipfel in Stuttgart Politik fordert mehr Sicherheit im Netz	negativ
Sicherheit	Bauernfänger gibts natürlich im Netz, und dagegen kann man auch mit etwas Verstand seitens der User, sowie bestehenden Gesetzen ankommen. Vielmehr erwarte ich mehr Sicherheit vor Rechteverwertern, Hausdurchsuchungen, Vorratsdatenspeicherung, Zensur und der Abmahnindustrie.	08.12.2009	http://www.bbv-net.de/public/article/digitale/792926/Politik-fordert-mehr-Sicherheit-im-Netz.html	IT-Gipfel in Stuttgart Politik fordert mehr Sicherheit im Netz	negativ
Datenschutz	Und wissen wir nicht schon lange, dass die bösen Hacker (... Geldfälscher, Betrüger, Spione aus Leidenschaft, aus der Wirtschaft oder auch "legitime" Regierungsspione) immer einen Schritt voraus sind und erst nach einem GAU die Lücken (eventuell) ausgebessert werden?	14.12.2009	http://www.netzwelt.de/news/81391-elektronischer-personalausweis-chipkarte-kommt-jahr-2010.html	Bundesinnenministerium bestätigt Terminplan Elektronischer Personalausweis: Chipkarte kommt im Jahr 2010	negativ
Vertrauen	Also, solange der Gebrauch einer Mikrowelle erlaubt ist werde ich, sobald ich diesen Ausweis in den Händen halte selbigen damit behandeln.	15.12.2009	http://www.netzwelt.de/news/81391-elektronischer-personalausweis-chipkarte-kommt-jahr-2010.html	Bundesinnenministerium bestätigt Terminplan Elektronischer Personalausweis: Chipkarte kommt im Jahr 2010	negativ

Kategorie	Was	Wann	Wo	Artikelname	Meinungsbild
Vertrauen	Man nimmt einfach ein Stück Alu-Folie und wickelt die Karte darin ein. Wird eh selten gebraucht. Alternativ sollte es auch gehen wenn man die Karte in eine Mikrowelle für wenige Sekunden bestrahlt. Es gibt auch spezielle Portmonaies die die RFIDs abschirmen. Seit es diese gibt besitzen Portmonaies in meinen Augen eine wichtige Aufgabe mehr.	15.12.2009	http://www.netzwelt.de/news/81391-elektronischer-personalausweis-chipkarte-kommt-jahr-2010.html	Bundesinnenministerium bestätigt Terminplan Elektronischer Personalausweis: Chipkarte kommt im Jahr 2010	negativ
Recht	Kleine Information: Der Reisepass und dein Personalausweis sind Eigentum der Bundesrepublik Deutschland. Die Zerstörung vom RFID-Chip wäre demnach Sachbeschädigung. Außerdem hast du Probleme bei der Einreise in die Vereinigten Staaten. Wenn die Zöllner den Chip nicht lesen können nehmen sie vor Ort Fingerabdrücke.	15.12.2009	http://www.netzwelt.de/news/81391-elektronischer-personalausweis-chipkarte-kommt-jahr-2010.html	Bundesinnenministerium bestätigt Terminplan Elektronischer Personalausweis: Chipkarte kommt im Jahr 2010	positiv
Sicherheit	Also eins ist ganz klar, mein Perso bekommt SOFORT eine Micro-Dusche und wenn die Amis mir dafür Fingerabdrücke abnehmen werden, soll mir das 1000 mal lieber sein, als in Deutschland als "Funksignalgeber" für kriminelle durch die Stadt zu laufen !!!!!	15.12.2009	http://www.netzwelt.de/news/81391-elektronischer-personalausweis-chipkarte-kommt-jahr-2010.html	Bundesinnenministerium bestätigt Terminplan Elektronischer Personalausweis: Chipkarte kommt im Jahr 2010	negativ

Bedenken von Bürgern bezüglich des neuen Personalausweis Projekten in Deutschland

D. Teilnehmer der zentral koordinierten Anwendungstests

Name der Organisation	Testszenario
Air Berlin	Fluggastabfertigung
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)	E Government Services
Allianz Deutschland AG	Kundenserviceprozesse im Versicherungsportal
ARGE eKFZ (Fraunhofer FOKUS; Christoph Kroschke AG; subreport; BDR; versch. Verwaltungen)	Teilprojekte eKFZ, Metaportal eVergabe und Premium EA (EU-DLR)
Bayerisches Landesamt für Steuern	Registrierungsverfahren für ELSTER (elektronische Steuererklärung)
bird.i ag & co. kg	Zutrittskontrolle, Zeiterfassung, Besucherverwaltung, Check-In in Hotels
CosmosDirekt	authentisierte Willenserklärungen und Mitteilungen
Datenzentrale Baden-Würtemberg	Online Gewerbeanzeige des Kommunalen Gewerbemanagements
Deutsche Emissionshandelsstelle (DEHSt) im Umweltbundesamt	Antrag auf Zuteilung von Emissionszertifikaten und Emissionsberichterstattung
Deutsche Kreditbank	Online Banking
Deutsche Rentenversicherung	eService der Deutschen Rentenversicherung
d-hosting GmbH	E Government Services
FRITZ & MACZIOL GmbH	elektronische Verwaltung von Entsorgungsnachweisen und Begleitscheinen
Fujitsu Technology Solutions	Fujitsu Online Shop Deutschland
Gothaer Allgemeine Versicherung	Antragstellung
Hagener E-Governmentkonsortium (Stadt Hagen; HABIT; Fernuniversität Hagen; IKS GmbH der FU Hagen, IFG CC, SAP)	Kommunale Verwaltungsdienstleistungen aus dem E Government Framework des virtuellen Rathaus 21
HSH Soft- und Hardware Vertriebs GmbH	E Bürgerservice
HUK24	Online-Versicherung
init AG in Zusammenarbeit mit der Arbeitsgruppe Extrapol	Unterstützung der länderübergreifenden Zusammenarbeit der Polizei Rahmen der gemeinsamen Plattform "Extrapol"
InterCard AG	Kundenkarte mit Zahlfunktion
Lotterie-Treuhandgesellschaft	Registrierung und Altersverifikation für Glücksspiele
LVM-Versicherungen	Authentifizierung, Portalzugang, Adressübernahme
Provinzial Rheinland	Versicherungsbeantragung
Schufa	Verbraucher-Onlineportal meineschufa.de und Online-Beantragung von Eigenauskünften
SIZ – Informatikzentrum der Sparkassenorganisation	Online-Beantragung von qualifizierten elektronischen Signaturen
Tönjes Holding AG	Identitätsnachweis bei Online-Zulassungen von Kfz
T-Systems Enterprise Services in Kooperation mit Innenministerium Baden-Württemberg:	"mein service-bw" im Verwaltungsdiensteportal Baden-Württemberg
Verkehrsverbund Rhein-Ruhr	eTicket-System
Willi Weber GmbH & Co. KG	Altersverifikation an Zigarettenautomaten

Wincor Nixdorf International	Authentifizierung an Geldautomaten oder Transaktionsterminals in Banken, Behörden und Industrie

E. Liste von Unternehmen, die für Anwendungstests ausgewählt wurden (Ausschnitt)

Name der Organisation	Testszenario
AHB Systeme GmbH	Zutrittskontrolle und Zeiterfassung
RESISTO IT GmbH	Altersverifikation im Internet
bremen online services GmbH & Co. KG	Elektronisches Gerichts- und Verwaltungspostfach (EGVP)
Landratsamt Calw	E-Bürgerdienste, wie Führerschein online, Online-Kfz-Zulassung, Online-Bauantrag
SEIB Peter Cornelius GmbH	Zugang zu Ausschreibungsinformationen
Humboldt-Universität zu Berlin, Institut für Informatik	Einschreibung zum Informatikstudium und Accountverwaltung mit Passwortrecovery
Stadt Dortmund	Virtuelles Rathaus
procilon IT-Logistics GmbH	Bauantragsverfahren, Registrierungs- und Metadatendienst EU-DLR, Authentifizierung, Kfz-Auskunft
petaFuel GmbH	PrnPAid MasterCard
WIBU-SYSTEMS AG	Vertrieb und Lizenzierung von Software, Dokumenten und Medien mit anwenderfreundlichen digitalen Rechtemanagement
quattro research GmbH	Personenidentifikation zum Erfindungsnachweis für Patente
Kästner Sicherheitstechnik	Zutrittskontrolle
AKDB Anstalt für Kommunale Datenverarbeitung in Bayern	Führerscheinverfahren OK.EFA; Einwohnerwesen OK.EWO; Zentrale Einfache Melderegisterauskunft ZEMA
bbg Betriebsberatungs GmbH	Single Sign On in der Versicherungswirtschaft
Ricoh International B.V.	Digitale Kopier- und Druckmaschinen
signalkontor GmbH	Passwort Manager für Windows und den Internet Explorer
e-data GmbH	Zutrittskontrolle
NetzWerkPlan GmbH	Planverwaltung im Projektkommunikationsraum, hier "Verbindliche Freigabe von planungsrelevanten Plänen und Dokumenten"
impuls systems GmbH	Rechtsgültiger Abschluss von Versicherungen On- und Offline
Akademische Arbeitsgemeinschaft Wolters Kluwer Deutschland GmbH	Authentifizierung für ELSTER, Banking-Anwendungen
it's me! GmbH	Portal zum nutzergesteuerten Identitätsmanagement
FaxLogic Gesellschaft für Kommunikationslösungen mbH	Single Sign On im Gesundheitswesen und Single Sign On im Versicherungswesen
ValiPic (Deutschland) GmbH; Centralverband der Berufsphotographen	Elektronische Übermittlung von Lichtbildern von Fotografen zu Meldestellen
vita-X AG	Zugangsschlüssel zur elektronischen Gesundheitsakte
Finanzbehörde Hamburg	Identitätsnachweis
Klinikum Ingolstadt	Patientenaufnahme, -identifikation
Mentana-Claimsoft AG	Sichere Identifizierung für De-Ident und andere Platt-

	formen
BIG Gesundheit - Die Direktkrankenkasse	BIGexclusiv
RISER ID Services GmbH	RISER ID Check
communal.cc	Wissens- und Kontaktmanagementsystem
EMC Deutschland GmbH	Zugang zu EMC Kunden Supportportalen (Powerlink, eFraud) und webbasierter Backupinfrastruktur (MOZY)
MATERNA GmbH Information & Communications	Unternehmensweites Identity-Management für den Mittelstand
Ministerium des Inneren des Landes Sachsen-Anhalt	e-shop-System Landesverwaltung Sachsen-Anhalt
iC Consult GmbH	Authentisierungsdienste in Unternehmensverzeichnissen
SERVODATA GmbH und Sperr e. V. Verein zur Förderung der Sicherheit in der Informationsgesellschaft	Sperr-Notruf 116 116
ARGE Car on Demand	Car on Demand, standortunabhängiges- Vermieter-übergreifendes Nutzungssystem für Mietwagen
Scholz Systemprogrammierung GmbH	Zugangs- und Alterskontrolle für Gebäude und Automaten
Finanzministerium Schleswig-Holstein	Schleswig-Holstein-Service
Fraunhofer IPK	Identifizierung mit dem elektronischen Personalausweis für die effiziente Verbundforschung innerhalb der Fraunhofer Gesellschaft
IMP Computersysteme AG in Zusammenarbeit mit dem Institut für Transfusionsmedizin der Universitätsklinik Köln	Blutspender-Identifizierung
LOTTO Hamburg GmbH	1) Einmalige Kundenregistrierung/Identifizierung 2) Laufende Authentisierung (Offline/Online) 3) Personalisierte Serviceangebote (Offline/Online) 4) Öffentliche elektronische Infrastruktur
bol Behörden Online Systemhaus GmbH	Diverse Online-Antragsverfahren im Rahmen bereits existierender E-Government-Anwendungen
mps public solutions GmbH	e-Bürgerdienste, u. a. Online-Wahlscheinantrag, einfache Melderegisterauskunft
Bundesdruckerei GmbH	ID Provider
Ingenieuris GmbH	Zertifizierungs-/Akkreditierungstellen ISO9001, Dokumentation sicherheitsrelevanter/-kritischer Daten und Vorgänge in Produktionsbereichen
ERGO Versicherungsgruppe	1) Internet-Login 2) Online-Anfrage für Lebens- und Rentenversicherungen
DGN Deutsches Gesundheitsnetz Service Gmb	Online-Beantragung qualifizierter Signaturen und Anmeldung am Online-Dienst „Deutsches Gesundheitsnetz“
ITSG GmbH	ELENA - Registratur Fachverfahren (vorbehaltlich des Abschlusses im Gesetzgebungsverfahren)
F1 GmbH in Zusammenarbeit mit der Euronorm GmbH	Identitätsnachweis unter Nutzung des nPA bei der Anmeldung und Nutzung des Portals PROTON
SAP Deutschland AG & Co. KG in Partnerschaft mit idematrix GmbH	Automatisierte Verifikation der Identität des physischen Besitzers im Rahmen von Services wie Ticketing, Fluggastabfertigung, Bezahldienste, Zugang zu Netzwerken , Daten und Objekten
digitronic computersysteme GmbH	Internetzugang in Computerpools von Hochschulen
ubinova UG (haftungsbeschränkt) & Co. KG	Event-ID-Management
Haas IT GmbH	e-Ticketing mit ÖPNV, bei Events und Zutrittskontrollen
media transfer AG	Altersverifikation im Internet gem. KJM Anforderun-

	gen, Registrierung/Identifizierung bei Portalen
Stadt Herzogenrath (mit Fa. FormSolutions)	Elektronische Formulare
Direct Center Kommunikationssysteme Knoll GmbH	Plattform Datenschutz im Direktmarketing - "Sichere Adresse"
BÜROTEX GmbH	SystemhausOnline Shop
Nordrheinische Ärzteversorgung	2-Faktor Authentifizierung mit nPA und Online Rentensimulation/Mitglieder-Portal
Hewlett-Packard GmbH (HP)	Internetkundenportal des Landesamtes für Besoldung und Versorgung des Landes Baden-Württemberg
bremen online services GmbH & Co. KG	Governikus Integrationswebservice und Bürgerclient
intarsys consulting GmbH	Elektronische Patientenakte - Arzt zu Arzt, Arzt zu Patient
Wrocklage Intermedia GmbH Aloaha Software	Software für Smartkarten
Niedersächsisches Ministerium für Inneres, Sport und Integration	Zentraler Identitätsmanagement Dienst (ZIMD) des Landes Niedersachsen
Clavid AG	Internet Identity Provider (OpenID und SAML)
Hessisches Ministerium des Innern und für Sport	Online-Antragstellung im Rahmen des Vorhabens "Einführung von Formularmanagement"
Landeshauptstadt Stuttgart, Kommunales Rechenzentrum der Region Stuttgart, KIND w.V.	Einmal registrieren, Immer Identifizieren (ERII) Interoperabilität portalübergreifender Identifizierung
Hessisches Landesamt für Straßen- und Verkehrswesen (HLSV)	VEMAGS - Das bundeseinheitliche Verfahrensmanagement für Großraum- und Schwertransporte der Länder und des Bundes
Net of Trust an der Universität der Bundeswehr München	Zugang auf Informationsportale
Gutwirth, Lauterbach u. Liebig GbR	Onlineshop, Bestellung von Fashion- bzw. Sportprodukten
Sascha Diebel EK	Internet-Identifikation für Webseiten mit Altersverifikation
Duale Hochschule Baden-Württemberg Mannheim	Zugangskontrolle für Netzwerke und User-Self-Services
Boll und Partner Software GmbH	E-Government-Lösungen mit digitaler Signatur und Identitätsnachweis
SecCommerce Informationssysteme GmbH	Integration des nPA in Software zur elektronischen Authentifizierung und qualifizierten elektronischen Signatur, u. a. für eService-DRV
Duisburg Verkehrsgesellschaft AG in Kooperation mit der Essener Verkehrs AG und Mühlheimer Verkehrsgesellschaft mbH (rrp-Verkehr)	Customer-Self-Care Terminals (CSC-Terminals)
VOICETRUST AG	Authentifizierung mit Sprecherverifikation, z.B. telefonischer Self-Service-PIN-Reset
PPI AG	Authentifizierung und Autorisierung im Umfeld e-Banking
Secaron AG	Authentisierungsdienste/Identifizierungsdienste in Netzwerkinfrastrukturen (z. B. Zugang über RAS-Gateway durch externe Mitarbeiter)
Kommunale Datenverarbeitungszentrale Citkomm, Iserlohn	Authentifizierung von Bürgern und Unternehmen für den Zugriff auf E-Government-Dienstleistungen
Versicherungswirtschaftlicher Datendienst	Authentifizierung und Single Sign-on von Versicherungsmaklern für Zugriff auf Web Services von Versicherungsunternehmen
Telecomputer GmbH	Fahrzeug-Zulassung (IKOL-KFZ), Fahrerlaubniswesen (IKOL-FS)
Sagem Monetel GmbH	Zertifikatseinbringung für ELENA Verfahren
NÜRNBERGER Versicherungsgruppe	Authentifizierung - Registrierung ExtraNet
komuna GmbH	Rathaus Service-Portal

van den Berg Consulting & Service AG	Bereitstellung eCard-API-Middleware
Zurich Versicherung	Kunden Selbstservice-Portal
DATEV eG	Online-Zugriff auf Lohn- und Gehaltsabrechnungen
Bundesministerium des Innern, Geschäftsstelle Deutschland-Online	Wissensplattform für den IT-Planungsrat
Defense AG	Informationssicherheit, Content sowie Websecurity, Zugangs- und Accesskontrolle
Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)	Single-Sign-On für ungebundene Vermittler
fun communications GmbH	Kombination von benutzerzentrierten Identitätsverfahren mit dem nPA zur erweiterten Identifikation
BillSAFE GmbH	Online-Factoring, Internetservice
novedia finance software ag	Identifizierung im Online Banking
FlexSecure GmbH	InSel - Informationelle Selbstbestimmung in Dienstenetzen
Hochschule Coburg	Hochschulweites Single Sign-On
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Zugriff auf digitale Daten im Internet der Dinge
AXA Konzern AG	Authentifizierungsverfahren im Maklerportal/-extranet der AXA
Funk-Sicherungs-Club NRW e. V.	Überprüfung der Zugangsberechtigung auf Veranstaltungen
Technische Universität Darmstadt	nPA-gestützte Authentisierung mit dem Handy
Universität Koblenz-Landau	Registrierung von digitalen Signaturzertifikaten
Fraunhofer Institut SIT	Sicheres VoIP zur Eröffnung eines Bankkontos (nur für Demonstrationszwecke)
CompuGROUP Holding AG	Elektronische Gesundheitsakten
Nokia Siemens Networks	Mobile Nutzung des nPA
MATESO GmbH	Zugang zur Software und zu gespeicherten Daten nach Identifizierung des Anwenders mittels der Personalausweisdaten
Verlag für Standesamtswesen GmbH	Onlineurkundenservice
Stadt Wolfsburg	Selbstregistrierung am Portal der Stadt Wolfsburg zur Nutzung von E-Governmentdiensten
Hochschule Darmstadt, Fachbereich Informatik	eID-Authentifizierung für vertrauliche Voice-over-IP-Telefonate
B+S Banksysteme Aktiengesellschaft	Online-Banking (Authentifizierung), Kontoeröffnung (Identifikation)
Bonk Consulting GmbH	ORWELL DMS (Direktmarketingserver) Provider
Württembergische Gemeinde-Versicherung a.G. und die WGV-Versicherung AG	Authentifizierung Portalzugang, Antragstellung und Online-Versicherung
fr-wlan GmbH	Verwaltung von lokalen Wlan-Netzwerken
DATA BECKER GmbH & Co KG	Einbindung nPA in "shop to date": Software zur Erstellung von online-shops; Nutzung des Verfahrens für

	den hauseigenen onlineshop unter www.databecker.de
D-TRUST GmbH	Beantragung und Ausgabe von QES-Karten am Online-Registrierungsarbeitsplatz (Online-RA)
ICT Europe GmbH	Jugendschutz an Verkaufsautomaten wie z.B. Zigarettenautomaten
BSI/Projekt STORK	Europäische E-Government-Portale und in Deutschland mein-service-BW
Bibliothek der TH (FH) Wildau	Bibliotheksbenutzerausweis für extern, nicht der TH Wildau angehörige Bibliothekskunden
VZnet Netzwerke Ltd. Berlin	Soziale Netzwerke schülerVZ, studiVZ und meinVZ
Gerrit Albrecht	API zur Nutzung der Funktionen des nPA
Hannoversche Lebensversicherung AG	Online-Antragsverfahren für Versicherungen
Reiner Kartengeräte GmbH & Co. KG	Individualshops für Banken, Sparkassen, Trust Center etc.
Stuttgarter Lebensversicherung a.G.	Single Sign On
highQ Computersysteme GmbH	Ticketing für den öffentlichen Personenverkehr (ÖPV)
Vodafone D2 GmbH	Auftragsformular für Telekommunikationsverträge
TeamDrive Systems GmbH	Virtuelle Server für die sichere Zusammenarbeit und den verschlüsselten Dokumentenaustausch für Unternehmen und Privatpersonen
Universität des Saarlandes, Lehrstuhl für Sicherheit und Kryptographie, Prof. Dr. Michael Backes	anonyme Beweistechniken auf der Basis der im Personalausweis gespeicherten Daten
IBM Deutschland GmbH	eID Service Integration in IBM SSO Sicherheitslösungen
infinity3 GmbH	Single-Sign-On für Online-Handel
SCM Microsystems GmbH	Internetbestellservice
Siemens AG, Siemens IT Solutions and Services	Show Case nPA-Formularmanagementsystem

F. Segmentierung der Anwendungstests nach Branche und Zielgruppe

Name der Einrichtung	Test-Szenario	Anwendungstests	Bereich (e-Gov, e-Business,	X2X (G2B, G2C, B2B, C2C, usw.)	Sektor
FRITZ & MACZIOL GmbH	elektronische Verwaltung von Entsorgungsnachweisen und Begleitscheinen	zentral	e-Gov	G2B, G2C	Abfallwirtschaft
procilon IT-Logistics GmbH	Bauantragsverfahren, Registrierungs- und Metadatendienst EU-DLR, Authentifizierung, Kfz-Auskunft	offen	e-Gov	G2C	Antragswesen
D-TRUST GmbH	Beantragung und Ausgabe von QES-Karten am Online-Registrierungsarbeitsplatz (Online-RA)	offen	e-Gov	G2C	Antragswesen
bol Behörden Online Systemhaus GmbH	Diverse Online-Antragsverfahren im Rahmen bereits existierender eGovernment-Anwendungen	offen	e-Gov	G2C	Antragswesen
Stadt Herzogenrath (mit Fa. FormSolutions)	Elektronische Formulare	offen	e-Gov	G2B, G2C	Antragswesen
AKDB Anstalt für Kommunale Datenverarbeitung in Bayern	Führerscheinverfahren OK.EFA; Einwohnerwesen OK.EWO; Zentrale Einfache Melderegisterauskunft ZEMA	offen	e-Gov	G2C	Antragswesen
Tönjes Holding AG	Identitätsnachweis bei Online-Zulassungen von Kfz?	zentral	e-Gov	B2B, B2C	Antragswesen
Hessisches Ministerium des Innern und für Sport	Online-Antragstellung im Rahmen des Vorhabens "Einführung von Formularmanagement"	offen	e-Gov	G2B, G2C	Antragswesen
ARGE eKFZ (Fraunhofer FOKUS; Christoph Kroschke AG; subreport; BDR; versch. Verwaltungen)	Teilprojekte eKFZ, Metaportal eVergabe und Premium EA (EU-DLR)	zentral	e-Gov	G2B, G2C	Antragswesen
SEIB Peter Cornelius GmbH	Zugang zu Ausschreibungsinformationen	offen	e-Gov	G2B	Ausschreibung
ARGE Car on Demand	Car on Demand, standortunabhängiges-Vermieterübergreifendes Nutzungssystem für Mietwagen	offen	e-Business	B2C	Automobil
Wincor Nixdorf International	Authentifizierung an Geldautomaten oder Transaktionsterminals in Banken, Behörden und Industrie	zentral	e-Business	B2C	Banken
PPI AG	Authentifizierung und Autorisierung im Umfeld eBanking	offen	e-Business	B2C	Banken
novedia finance software ag	Identifizierung im Online Banking	offen	e-Business	B2C	Banken
Reiner Kartengeräte GmbH & Co. KG	Individualshops für Banken, Sparkassen, Trust Center etc.	offen	e-Business	B2C	Banken
Deutsche Kreditbank, novedia finance software ag(oder andere)	Online Banking	zentral	e-Gov, e-Business	G2B, G2C	Banken
B+S Banksysteme Aktiengesellschaft	Online-Banking (Authentifizierung), Kontoeröffnung (Identifikation)	offen	e-Business	B2C	Banken
SIZ – Informatikzentrum der Sparkassenorganisation	Online-Beantragung von qualifizierten elektronischen Signaturen	zentral	e-Business	B2B, B2C	Banken
petaFuel GmbH	Prepaid MasterCard	offen	e-Business	B2C	Banken
Fraunhofer Institut SIT	Sicheres VoIP zur Eröffnung eines Bankkontos (nur für Demonstrationszwecke)	offen	e-Business	B2C	Banken
T-Systems Enterprise Services in Kooperation mit Innenministerium Baden-Württemberg:	"mein service-bw" im Verwaltungsdiensteportal Baden-Württemberg	zentral	e-Gov	G2B, G2C	Bundesland
ubinova UG (haftungsbeschränkt) & Co. KG	Event-ID-Management	offen	e-Business	B2C	Event
ITSG GmbH	ELENA - Registratur Fachverfahren (vorbehaltlich des Abschlusses im Gesetzgebungsverfahren)	offen	e-Gov	G2B, G2C, B2C	Finanzen
Finanzbehörde Hamburg	Identitätsnachweis	offen	e-Gov	G2C	Finanzen
Hewlett-Packard GmbH (HP)	Internetkundenportal des Landesamtes für Besoldung und Versorgung des Landes Baden-Württemberg	offen	e-Gov	G2C	Finanzen
BillSAFE GmbH	Online-Factoring, Internetservice	offen	e-Business	B2C	Finanzen
DATEV eG	Online-Zugriff auf Lohn- und Gehaltsabrechnungen	offen	e-Business	B2C	Finanzen
Finanzministerium Schleswig-Holstein	Schleswig-Holstein-Service	offen	e-Gov	G2C	Finanzen
Schufa	Verbraucher-Onlineportal meineschufa.de und Online-Beantragung von Eigenauskünften	zentral	e-Business	B2B, B2C	Finanzen
ValiPic (Deutschland) GmbH; Centralverband der Berufsphotographen	Elektronische Übermittlung von Lichtbildern von Fotografen zu Meldestellen	offen	e-Gov	G2B	Fotografie
Nordrheinische Ärzteversorgung	2-Faktor Authentifizierung mit ePA und Online Rentensimulation / Mitglieder-Portal	offen	e-Gov, e-Business	G2B	Gesundheit
BIG Gesundheit - Die Direktkrankenkasse	BIGexclusiv	offen	e-Business	B2C	Gesundheit
IMP Computersysteme AG in Zusammenarbeit mit dem Institut für Transfusionsmedizin der Universitätsklinik Köln	Blutspender-Identifizierung	offen	e-Gov, e-Business	G2B	Gesundheit
CompuGROUP Holding AG	Elektronische Gesundheitsakten	offen	e-Business	B2B, B2C	Gesundheit
intarsys consulting GmbH	Elektronische Patientenakte - Arzt zu Arzt, Arzt zu Patient	offen	e-Business	B2B, B2C	Gesundheit
DGN Deutsches Gesundheitsnetz Service GmbH	Online-Beantragung qualifizierter Signaturen und Anmeldung am Online-Dienst „Deutsches Gesundheitsnetz“	offen	e-Business	B2B, B2C	Gesundheit
Klinikum Ingolstadt	Patientenaufnahme, -identifikation	offen	e-Business	B2C	Gesundheit
FaxLogic Gesellschaft für Kommunikationslösungen mbH	Single Sign On im Gesundheitswesen	offen	e-Business	G2C, B2C	Gesundheit
vita-X AG	Zugangsschlüssel zur elektronischen Gesundheitsakte	offen	e-Business	B2C, C2C	Gesundheit

Name der Einrichtung	Test-Szenario	Anwendungstests	Bereich (e-Gov, e-Business,	X2X (G2B, G2C, B2B, C2C, usw.)	Sektor
LOTTO Hamburg GmbH	1) Einmalige Kundenregistrierung / Identifizierung 2) Laufende Authentisierung (Offline / Online) 3) Personalisierte Serviceangebote (Offline / Online) 4) Öffentliche elektronische Infrastruktur	offen	e-Business	B2C	Glücksspiel
Lotterie-Treuhandgesellschaft	Registrierung und Altersverifikation für Glücksspiele	zentral	e-Business	B2C	Glücksspiel
RESISTO IT GmbH	Altersverifikation im Internet	offen	e-Business	B2C	Handel
DATA BECKER GmbH & Co KG	Einbindung nPA in "shop to date": Software zur Erstellung von online-shops; Nutzung des Verfahrens für den hauseigenen onlineshop unter www.databecker.de	offen	e-Business	B2C	Handel
Ministerium des Inneren des Landes Sachsen-Anhalt	e-shop-System Landesverwaltung Sachsen-Anhalt	offen	e-Gov	G2C	Handel
Fujitsu Technology Solutions	Fujitsu Online Shop Deutschland	zentral	e-Business	B2B, B2C	Handel
Intercard AG	Kundenkarte mit Zahlfunktion	zentral	e-Business	B2C	Handel
Gutwirth, Lauterbach u. Liebig GbR	Onlineshop, Bestellung von Fashion- bzw. Sportprodukten	offen	e-Business	B2C	Handel
Bonk Consulting GmbH	ORWELL DMS (Direktmarketingserver) Provider	offen	e-Business	B2C	Handel
RISER ID Services GmbH	RISER ID Check	offen	e-Business	B2C	Handel
EMC Deutschland GmbH	Zugang zu EMC Kunden Supportportalen (Powerlink, eFraud) und webbasierter Backupinfrastruktur (MOZY)	offen	e-Business	B2C	Handel
Gerrit Albrecht	API zur Nutzung der Funktionen des ePA	offen	e-Gov, e-Business	G2B, B2B	Information
HSH Soft- und Hardware Vertriebs GmbH	E Bürgerservice	zentral	e-Gov	G2C	Information
d-hosting GmbH	E Government Services	zentral	e-Gov	G2B, G2C	Information
BSI / Projekt STORK	Europäische eGovernment-Portale und in Deutschland mein-service-BW	offen	e-Gov	G2B, G2C	Information
Defense AG	Informationssicherheit, Content sowie Websecurity, Zugangs- und Accesskontrolle	offen	e-Business	B2C	Information
FlexSecure GmbH	InSel - Informationelle Selbstbestimmung in Dienstenetzen	offen	e-Gov	G2C	Information
komuna GmbH	Rathaus Service-Portal	offen	e-Gov	G2B, G2C	Information
Stadt Dortmund	Virtuelles Rathaus	offen	e-Gov	G2B, G2C	Information
communal.cc	Wissens- und Kontaktmanagementsystem	offen	e-Gov	G2C	Information
Bundesministerium des Innern, Geschäftsstelle Deutschland-Online	Wissensplattform für den IT-Planungsrat	offen	e-Gov	G2G	Information
Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Zugriff auf digitale Daten im Internet der Dinge	offen	e-Business	B2C	Information
VZnet Netzwerke Ltd. Berlin	Soziale Netzwerke schülerVZ, studiVZ und meinVZ	offen	e-Business	B2C	Internet
fr-wlan GmbH	Verwaltung von lokalen Wlan-Netzwerken	offen	e-Business	B2B, B2C	Internet
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)	E Government Services	zentral	e-Gov	G2B, G2C	Kommune
Landratsamt Calw	E-Bürgerdienste, wie Führerschein online, Online-Kfz-Zulassung, Online-Bauantrag	offen	e-Gov	G2C	Kommune
Hagener E-Governmentkonsortium (Stadt Hagen; HABIT; Fernuniversität Hagen; IKS GmbH der FU Hagen, IFG CC, SAP)	Kommunale Verwaltungsdienstleistungen aus dem E Government Framework des virtuellen Rathaus 21	zentral	e-Gov	G2B, G2C	Kommune
Datenzentrale Baden-Würtemberg	Online Gewerbeanzeige des Kommunalen Gewerbemanagements	zentral	e-Gov	G2B	Kommune
SAP Deutschland AG & Co. KG in Partnerschaft mit idematrix GmbH	Automatisierte Verifikation der Identität des physischen Besitzers im Rahmen von Services wie Ticketing, Fluggastabfertigung, Bezahldienste, Zugang zu Netzwerken , Daten und Objekten	offen	e-Business	B2C	Luftfahrt
Mentana-Claimsoft AG	Sichere Identifizierung für De-Ident und andere Plattformen	offen	e-Gov	G2C	Mail
Technische Universität Darmstadt	ePA-gestützte Authentisierung mit dem Handy	offen	e-Gov	G2C	Mobilfunk
NetzWerkPlan GmbH	Planverwaltung im Projektkommunikationsraum, hier "Verbindliche Freigabe von planungsrelevanten Plänen und Dokumenten"	offen	e-Gov	G2B, G2C	Planung
init AG in Zusammenarbeit mit der Arbeitsgruppe Extrapol	Unterstützung der länderübergreifenden Zusammenarbeit der Polizeien Rahmen der gemeinsamen Plattform "Extrapol"	zentral	e-Gov	G2G	Polizei
Ingenieuris GmbH	Zertifizierungs-/Akkreditierungstellen ISO9001, Dokumentation sicherheitsrelevanter/-kritischer Daten und Vorgänge in Produktionsbereichen	offen	e-Business	B2B	Produktion
media transfer AG	Altersverifikation im Internet gem. KJM Anforderungen, Registrierung/Identifizierung bei Portalen	offen	e-Business	B2C	Recht
Kommunale Datenverarbeitungszentrale Citkomm, Iserlohn	Authentifizierung von Bürgern und Unternehmen für den Zugriff auf E-Government-Dienstleistungen	offen	e-Gov	G2B, G2C	Recht
CosmosDirekt	authentisierte Willenserklärungen und Mitteilungen	zentral	e-Business	B2C	Recht
Secaron AG	Authentisierungsdienste / Identifizierungsdienste in Netzwerkinfrastrukturen (z. B. Zugang über RAS-Gateway durch externe Mitarbeiter)	offen	e-Business	B2C	Recht
mps public solutions GmbH	e-Bürgerdienste, u. a. Online-Wahlscheinantrag, einfache Meldregisterauskunft	offen	e-Gov	G2C	Recht
Boll und Partner Software GmbH	E-Government-Lösungen mit digitaler Signatur und Identitätsnachweis	offen	e-Gov	G2B, G2C	Recht
Landeshauptstadt Stuttgart, Kommunales Rechenzentrum der Region Stuttgart, KIND w.V.	Einmal registrieren, Immer Identifizieren (ERII) Interoperabilität portalübergreifender Identifizierung	offen	e-Gov	G2B, G2C	Recht
bremen online services GmbH & Co. KG	Elektronisches Gerichts- und Verwaltungspostfach (EGVP)	offen	e-Gov	G2B, G2C	Recht

Name der Einrichtung	Test-Szenario	Anwendungstests	Bereich (e-Gov, e-Business,	X2X (G2B, G2C, B2B, C2C, usw.)	Sektor
bremen online services GmbH & Co. KG	Governikus Integrationswebservice und Bürgerclient	offen	e-Gov	G2C	Recht
Hochschule Coburg	Hochschulweites Single Sign-On	offen	e-Gov	G2C	Recht
Bundesdruckerei GmbH	ID Provider	offen	e-Gov	G2B, G2C	Recht
Fraunhofer IPK	Identifizierung mit dem elektronischen Personalausweis für die effiziente Verbundforschung innerhalb der Fraunhofer Gesellschaft	offen	e-Business	B2C	Recht
F1 GmbH in Zusammenarbeit mit der Euronorm GmbH	Identitätsnachweis unter Nutzung des ePA bei der Anmeldung und Nutzung des Portals PROTON	offen	e-Gov, e-Business	G2C, B2C	Recht
SecCommerce Informationssysteme GmbH	Integration des ePA in Software zur elektronischen Authentifizierung und qualifizierten elektronischen Signatur, u. a. für eService-DRV	offen	e-Gov	G2C	Recht
Clavid AG	Internet Identity Provider (OpenID und SAML)	offen	e-Gov, e-Business	G2C, B2C	Recht
Sascha Diebel EK	Internet-Identifikation für Webseiten mit Altersverifikation	offen	e-Business	B2C	Recht
fun communications GmbH	Kombination von benutzerzentrierten Identitätsverfahren mit dem ePa zur erweiterten Identifikation	offen	e-Gov	G2C	Recht
Nokia Siemens Networks	Mobile Nutzung des nPA	offen	e-Business	B2C	Recht
quattro research GmbH	Personenidentifikation zum Erfindungsnachweis für Patente	offen	e-Gov	G2C	Recht
it's me! GmbH	Portal zum nutzergesteuerten Identitätsmanagement	offen	e-Business	B2C	Recht
Universität Koblenz-Landau	Registrierung von digitalen Signaturzertifikaten	offen	e-Gov	G2C	Recht
Wrocklage Intermedia GmbH Aloaha Software	Software für Smartkarten	offen	e-Business	B2C	Recht
Niedersächsisches Ministerium für Inneres, Sport und Integration	Zentraler Identitätsmanagement Dienst (ZIMD) des Landes Niedersachsen	offen	e-Gov	G2C	Recht
Scholz Systemprogrammierung GmbH	Zugangs- und Alterskontrolle für Gebäude und Automaten	offen	e-Business	B2C	Recht
Duale Hochschule Baden-Württemberg Mannheim	Zugangskontrolle für Netzwerke und User-Self-Services	offen	e-Business	B2C	Recht
Kästner Sicherheitstechnik	Zutrittskontrolle	offen	e-Gov, e-Business	G2B, G2C	Recht
e-data GmbH	Zutrittskontrolle	offen	e-Gov, e-Business	G2B, G2C	Recht
AHB Systeme GmbH	Zutrittskontrolle und Zeiterfassung	offen	e-Gov, e-Business	G2B, G2C	Recht
SERVODATA GmbH und Sperr e. V. Verein zur Förderung der Sicherheit in der Informationsgesellschaft	Sperr-Notruf 116 116	offen	e-Gov, e-Business	G2B, G2C, B2C	Sicherheit
iC Consult GmbH	Authentisierungsdienste in Unternehmensverzeichnissen	offen	e-Gov, e-Business	G2B, B2B, B2C	Software
van den Berg Consulting & Service AG	Bereitstellung eCard-API-Middleware	offen	e-Gov	G2C	Software
Ricoh International B.V.	Digitale Kopier- und Druckmaschinen	offen	e-Business	B2C	Software
signalkontor GmbH	Passwort Manager für Windows und den Internet Explorer	offen	e-Business	B2C	Software
MATERNA GmbH Information & Communications	Unternehmensweites Identity-Management für den Mittelstand	offen	e-Business	B2B, B2C	Software
WIBU-SYSTEMS AG	Vertrieb und Lizenzierung von Software, Dokumenten und Medien mit anwenderfreundlichen digitalen Rechtemanagement	offen	e-Business	B2B, B2C	Software
MATESO GmbH	Zugang zur Software und zu gespeicherten Daten nach Identifizierung des Anwenders mittels der Personalausweisdaten	offen	e-Business	B2C	Software
Stadt Wolfsburg	Selbstregistrierung am Portal der Stadt Wolfsburg zur Nutzung von eGovernmentdiensten	offen	e-Gov	G2B, G2C	Stadt
Akademische Arbeitsgemeinschaft Wolters Kluwer Deutschland GmbH	Authentifizierung für ELSTER, Banking-Anwendungen	offen	e-Gov	G2B, G2C	Steuer
Bayerisches Landesamt für Steuern	Registirierungsverfahren für ELSTER	zentral	e-Gov	G2B, G2C	Steuer
Sagem Monetel GmbH	Zertifikatseinbringung für ELENA Verfahren	offen	e-Gov	G2B, G2C	Steuer
Willi Weber GmbH & Co. KG	Altersverifikation an Zigarettenautomaten	zentral	e-Business	B2C	Tabak
ICT Europe GmbH	Jugendschutz an Verkaufsautomaten wie z.B. Zigarettenautomaten	offen	e-Business	B2C	Tabak
Vodafone D2 GmbH	Auftragsformular für Telekommunikationsverträge	offen	e-Business	B2C	Telekommunikation
VOICETRUST AG	Authentifizierung mit Sprecherverifikation, z.B. telefonischer Self-Service-PIN-Reset	offen	e-Business	B2C	Telekommunikation
Hochschule Darmstadt, Fachbereich Informatik	eID-Authentifizierung für vertrauliche Voice-over-IP-Telefonate	offen	e-Business	B2B, B2C	Telekommunikation
Haas IT GmbH	e-Ticketing mit ÖPNV, bei Events und Zutrittskontrollen	offen	e-Business	B2C	Ticketing
Verkehrsverbund Rhein-Ruhr	eTicket-System	zentral	e-Business	B2C	Ticketing
highQ Computersysteme GmbH	Ticketing für den öffentlichen Personenverkehr (ÖPV)	offen	e-Gov	G2C	Ticketing
Funk-Sicherungs-Club NRW e. V.	Überprüfung der Zugangsberechtigung auf Veranstaltungen	offen	e-Business	B2C	Ticketing
bird.i ag & co. kg	Zutrittskontrolle, Zeiterfassung, Besucherverwaltung, Check-In in Hotels	zentral	e-Business	B2C	Ticketing
Duisburg Verkehrsgesellschaft AG in Kooperation mit der Essener Verkehrs AG und Mühlheimer Verkehrsgesellschaft mbH (rrp-Verkehr)	Customer-Self-Care Terminals (CSC-Terminals)	offen	e-Business	B2C	Transport

Name der Einrichtung	Test-Szenario	Anwendungstests	Bereich (e-Gov, e-Business,	X2X (G2B, G2C, B2B, C2C, usw.)	Sektor
Telecomputer GmbH	Fahrzeug-Zulassung (IKOL-KFZ), Fahrerlaubniswesen (IKOL-FS)	offen	e-Gov	G2C	Transport
Air Berlin	Fluggastabfertigung	zentral	e-Business	B2C	Transport
Hessisches Landesamt für Straßen- und Verkehrswesen (HLSV)	VEMAGS - Das bundeseinheitliche Verfahrensmanagement für Großraum- und Schwertransporte der Länder und des Bundes	offen	e-Gov	G2B	Transport
DEHSt im Umweltbundesamt	Antrag auf Zuteilung von Emissionszertifikaten und Emissionsberichterstattung	zentral	e-Gov	G2B	Umwelt
Bibliothek der TH (FH) Wildau	Bibliotheksbenutzerausweis für extern, nicht der TH Wildau angehörige Bibliothekskunden	offen	e-Gov	G2C	Universität
Humboldt-Universität zu Berlin, Institut für Informatik	Einschreibung zum Informatikstudium und Accountverwaltung mit Passwortrecovery	offen	e-Gov	G2C	Universität
digitronic computersysteme GmbH	Internetzugang in Computerpools von Hochschulen	offen	e-Gov	B2C	Universität
Net of Trust an der Universität der Bundeswehr München	Zugang auf Informationsportale	offen	e-Gov	G2C	Universität
Verlag für Standesamtswesen GmbH	Onlineurkundenservice	offen	e-Gov	G2C	Urkunde
Direct Center Kommunikationssysteme Knoll GmbH	Plattform Datenschutz im Direktmarketing - "Sichere Adresse"	offen	e-Business	B2B, B2C	Verkauf
BÜROTEX GmbH	SystemhausOnline Shop	offen	e-Business	B2C	Verkauf
ERGO Versicherungsgruppe	1) Internet-Login 2) Online-Anfrage für Lebens- und Rentenversicherungen	offen	e-Business	B2C	Versicherung
Gothaer Allgemeine Versicherung	Antragstellung	zentral	e-Business	B2C	Versicherung
NÜRNBERGER Versicherungsgruppe	Authentifizierung - Registrierung ExtraNet	offen	e-Business	B2B, B2C	Versicherung
Württembergische Gemeinde-Versicherung a.G. und die WGV-Versicherung AG	Authentifizierung Portalzugang, Antragstellung und Online-Versicherung	offen	e-Business	B2C	Versicherung
Versicherungswirtschaftlicher Datendienst	Authentifizierung und Single Sign-on von Versicherungsmaklern für Zugriff auf Web Services von Versicherungsunternehmen	offen	e-Business	B2B	Versicherung
LVM-Versicherungen	Authentifizierung, Portalzugang, Adressübernahme	zentral	e-Business	B2C	Versicherung
AXA Konzern AG	Authentifizierungsverfahren im Maklerportal / -extranet der AXA	offen	e-Business	B2B	Versicherung
Deutsche Rentenversicherung	eService der Deutschen Rentenversicherung	zentral	e-Gov, e-Business	G2B, G2C	Versicherung
Zurich Versicherung	Kunden Selbstservice-Portal	offen	e-Business	B2C	Versicherung
Allianz Deutschland AG	Kundenserviceprozesse im Versicherungsportal	zentral	e-Business	B2C	Versicherung
Hannoversche Lebensversicherung AG	Online-Antragsverfahren für Versicherungen	offen	e-Business	B2C	Versicherung
HUK24	Online-Versicherung	zentral	e-Business	B2B, B2C	Versicherung
impuls systems GmbH	Rechtsgültiger Abschluss von Versicherungen On- und Offline	offen	e-Business	B2C	Versicherung
Stuttgarter Lebensversicherung a.G.	Single Sign On	offen	e-Business	B2C	Versicherung
bbg Betriebsberatungs GmbH	Single Sign On in der Versicherungswirtschaft	offen	e-Business	B2C	Versicherung
Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)	Single-Sign-On für ungebundene Vermittler	offen	e-Business	B2B	Versicherung
Provinzial Rheinland	Versicherungsbeantragung	zentral	e-Business	B2C	Versicherung

G. Fragen im Vorschlag

Aufgabe	Details	Verant-wortlicher Partner	Behandelt in Ab-schnitt
Recherche und Auswertung der Literatur sowie Dokumentenanalyse (u.a. internationale Beispiel-Projekte) zur Herstellung von Vertrauen in nPA	Literatur- und Dokumentenauswertung zu Rahmenbedingungen sowie Konzepten, Methoden und Instrumenten der Herstellung von Vertrauen in Nutzung des nPA	TUM, Uni. St. Gallen	
Recherche und Auswertung der Literatur sowie Dokumentenanalyse (u.a. internationale Beispiel-Projekte) zur Gestaltung nach den Aspekten der Ergonomie und Einfachheit des Bürgerclients	Literatur- und Dokumentenauswertung zu Rahmenbedingungen sowie Konzepten, Methoden und Instrumenten zur Gestaltung nach den Aspekten der Ergonomie und Einfachheit des Bürgerclients	TUM	
Marktanalyse für den Bürgerclient (u.a. Branchen, Zielgruppe, Marktplayer, Konkurrenz, Marktvolumen, Markpotenzial)	Auswertung der Marktanalyse für den Bürgerclient	TUM	
Entwicklung der möglichen Geschäftsmodelle für den Bürgerclient durch Marktanalyse, Dokumentenanalyse, Interviews und Recherche	Mögliche Geschäftsmodelle für den Bürgerclient	TUM	
Identifizierung der Akteure und Ansprechpartner für jedes Geschäftsmodell	Liste von Akteuren, die bei einem Geschäftsmodell einzubinden sind und ihre Ansprechpartner	TUM	
Recherchieren der Projekte zu nPA/Bürgerclient in anderen Ländern hinsichtlich ihrer eingesetzten Geschäftsmodelle	Dokumentenauswertung der Geschäftsmodelle in anderen Ländern bei Projekten zu nPA/Bürgerclient	TUM	

LITERATUR

Adams, J. (1995): Risk: the policy impications of risk compensation and plural rationalities. UCL Press, London 1995.

Assar, S. B., I.; Boydens, I. (2011): Practical Studies in E-Government: Best Practices from Around the World. Springer Verlag, London 2011.

Bart, Y./ Shankar, V./ Sultan, F./ Urban, G. L. (2005): Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. In: Journal of Marketing, 69 (2005) 4, S. 133-152.

Bauer, R. A. (1967): Consumer Behavior as Risk Taking. In: Risk Taking and Information Handling in Consumer Behaviour. Ed.: Cox, D.F., Harvard University Graduate School of Business Administration, Boston 1967, S. 641-667.

Bayerisches Landesamt für Steuern (2010a): Information zu den Sicherheitsverfahren. In: https://www.elsteronline.de/eportal/Sicherheit.tax, zugegriffen am 01.02.2011.

Bayerisches Landesamt für Steuern (2010b): Statistische Auswertungen zur elektronischen Steuererklärung. In: https://www.elster.de/elster_stat_nw.php, zugegriffen am 06.12.2010.

Behörden Spiegel Online (2010): Neuer Personalausweis. In: http://www.behoerden-spiegel.de/Internet/nav/ef5/ef575b02-7e9d-921a-3b21-717b988f2ee2.htm, zugegriffen am 07.12.2010.

Belanger, F./ Hiller, J. S./ Smith, W. J. (2002): Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. In: The Journal of Strategic Information Systems, 11 (2002) 3-4, S. 245-270.

BITKOM (2009): Empfehlungen der ITK-Wirtschaft zur Einführung des elektronischen Personalausweises. In: http://www.bitkom.org/files/documents/Positionspapier_ePA_2009.pdf, zugegriffen am 07.02.2011.

Borchers, D. (2010a): AusweisApp zum neuen Personalausweis ausgeliefert. In: http://www.heise.de/security/meldung/AusweisApp-zum-neuen-Personalausweis-ausgeliefert-1128433.html, zugegriffen am 01.02.2011.

Borchers, D. (2010b): Banken zögern noch beim neuen Personalausweis In: http://www.heise.de/newsticker/meldung/Banken-zoegern-noch-beim-neuen-Personalausweis-1131584.html, zugegriffen am 31.03.2011.

Borchers, D. (2010c): Bundesinnenminister: Personalausweis für die Online-Welt ist sicher. In: http://www.heise.de/newsticker/meldung/Bundesinnenminister-Personalausweis-fuer-die-Online-Welt-ist-sicher-1127489.html, zugegriffen am 01.02.2011.

Bouma, T. (2006): Identity: setting the larger context and achieve the right outcomes In: http://www.cacr.math.uwaterloo.ca/conferences/2006/psw/Bouma.ppt, zugegriffen am 07.02.2011.

Bouwman, H. (2002): The sense and nonsense of Business Models. Paper presented at the International Workshop on Business Models, HEC Lausanne.

Bullinger, H.-L./ Scheer, A.-W. (2006): Service Engineering: Entwicklung und Gestaltung innovativer Dienstleistungen. 2. ed., Springer, Berlin, Heidelberg 2006.

Bundesamt für Sicherheit in der Informationstechnik (2005): Phasenplan E-Government. In: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Egovernment/3_Phase1_pdf.pdf;jsessionid=6D9436200F576FEA190C60F5996EE33E?__blob=publicationFile, zugegriffen am 26.01.2011.

Bundesamt für Sicherheit in der Informationstechnik (2010): Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe. In: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03104/BSI-TR-03104_V2_1_5_pdf.pdf?__blob=publicationFile, zugegriffen am 01.02.2011.

Bundesamt für Sicherheit in der Informationstechnik (2011a): Benötigte Software und Zertifikate - AusweisApp. In: https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Personalausweis/TechnischeGrundlagen/Software_Zertifikate/software_zertifikate_node.html, zugegriffen am 28.03.2011.

Bundesamt für Sicherheit in der Informationstechnik (2011b): Der neue Personalausweis - FAQ - Online-Ausweisfunktion. In: https://www.ausweisapp.bund.de/pweb/faq/faq.do?idbtn_faq:8:, zugegriffen am 28.03.2011.

Bundesamt für Sicherheit in der Informationstechnik (2011c): Von der AusweisApp unterstützte Lesegeräte. In: https://www.ausweisapp.bund.de/pweb/cms/kartenleser.jsp, zugegriffen am 13.05.2011.

Bundeskanzleramt Österreich (2005): Madrid: Bürgerkartenkonzept des Bundeskanzleramtes ausgezeichnet. In: http://www.bka.gv.at/site/4951/default.aspx#id14254, zugegriffen am 26.01.2011.

Bundeskanzleramt Österreich (2010): Bürgerkarte: Allgemeine Fragen. In: http://www.buergerkarte.at/haeufige-fragen.de.php, zugegriffen am 26.01.2011.

Bundesministerium der Justiz (2010a): §1 Ausweispflicht, Ausweisrecht. In: http://bundesrecht.juris.de/pauswg/__1.html, zugegriffen am 07.12.2010.

Bundesministerium der Justiz (2010b): §8 Auskunft an den Betroffenen. In: http://www.gesetze-im-internet.de/mrrg/__8.html, zugegriffen am 07.12.2010.

Bundesministerium des Inneren (2008): Einführung des elektronischen Personalausweises in Deutschland 2008.

Bundesministerium des Inneren (2009a): Registrierung und Teilnehmer am offenen Anwendungstest. In: http://www.cio.bund.de/DE/IT-Projekte/Neuer_Personalausweis/Registrierung_offener_Anwendungstest/registrierung_offener_anwendungstest_node.html, zugegriffen am 01.02.2011.

Bundesministerium des Inneren (2009b): Umsetzungsphase für den elektronischen Personalausweis beginnt. BMI gibt 30 Teilnehmer für den zentral koordinierten Anwendungstest bekannt. In: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2009/06/epa_anwendertest.html?nn=294838, zugegriffen am 05.03.2010.

Bundesministerium des Inneren (2010a): Begleitforschung. In: http://www.personalausweisportal.de/cln_164/DE/Der-Neue-Ausweis/Begleitforschung/begleitforschung_node.html, zugegriffen am 01.02.2011.

Bundesministerium des Inneren (2010b): Begleitstudien zum neuen Personalausweis. In: http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Begleitstudien/Begleitstudienstatement.pdf?__blob=publicationFile, zugegriffen am 19.01.2012.

Bundesministerium des Inneren (2010c): Das brauchen Sie um die Möglichkeiten des neuen Personalausweises nutzen zu können. In: http://www.personalausweisportal.de/cln_155/sid_9E5B5F1AEB877A551FDC381633F17E3F/DE/Neue-Moeglichkeiten/Das-brauchen-Sie/das-brauchen-sie_node.html, zugegriffen am 07.12.2010.

Bundesministerium des Inneren (2010d): Der neue Personalausweis - Steckbrief. In: http://www.personalausweisportal.de/cln_164/DE/Der-Neue-Ausweis/Steckbrief/steckbrief_node.html, zugegriffen am 29.11.2010.

Bundesministerium des Inneren (2010e): Fragen und Antworten. In: http://www.personalausweisportal.de/cln_164/DE/Der-Neue-Ausweis/Fragen-und-Antworten/faq_node.html, zugegriffen am 01.02.2011.

Bundesministerium des Inneren (2010f): Innovationen für eine eID-Architektur in Deutschland. In: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/Pressemappe_nPA/Innovationen_eID-Architektur_Deutschland.pdf?__blob=publicationFile, zugegriffen am 01.02.2011.

Bundesministerium des Inneren (2011): De-Mail – so einfach wie E-Mail, so sicher wie Papierpost. In: http://www.fn.de-mail.de/DeMail/DE/01_Buerger/Buerger_node.html, zugegriffen am 16.05.2011.

Bundesministerium für Familie (2009): Jugendschutzgesetz (JuSchG). In: http://www.bmfsfj.de/Kategorien/gesetze,did=5350.html, zugegriffen am 09.12.2009.

Bundesministerium für Wirtschaft und Technologie (2008): Dritter Nationaler IT-Gipfel: Stimmen der Arbeitsgruppen 3 und 4 zum Ausweisprojekt 2008.

Bundesministerium für Wirtschaft und Technologie (2009): 5. ePerformance Report 2009 IKT-Standort Deutschland im europäischen Vergleich. In:

http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/monitoring-iuk-5-performance-report,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, zugegriffen am 26.01.2011.

Bundesregierung (2008): Entwurf eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften.

Chadwick, S. A. (2001): Communicating trust in e-commerce interactions. In: Management Communication Quarterly, 14 (2001) 4, S. 653-658.

Chaos Computer Club e.V. (2005): Press Release of the Chaos Computer Club e.V. for the adoption of biometric Passports. In: http://dasalte.ccc.de/epass/CCC20051004?language=en, zugegriffen am 07.12.09.

Clarke, R. (1994): Human identification in information systems: management challenges and public policy issues. In: Information Technology & People, 7 (1994) 4, S. 6-37.

Commonwealth of Australia (2006): Model Criminal Code: Credit Card Skimming Offences 2006.

Culnan, M. J./ Armstrong, P. K. (1999): Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. In: Organization Science, 10 (1999) 1, S. 104-115.

Datenzentrale Baden-Württemberg (o. J.): KoGeMa. In: http://www.datenzentrale.de/servlet/PB/show/1269041/KoGeMa.pdf, zugegriffen am 07.12.2010.

Datenzentrale Baden-Württenmberg (2010): Der neue Personalausweis als Chance für kommunale Onlinedienste. In: http://www.datenzentrale.de/servlet/PB/show/1319360_l1/ModernerStaat_nPA_Tramer.pdf, zugegriffen am 01.02.2011.

Davis, F. D. (1989): Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. In: MIS Quarterly, 13 (1989) 3, S. 319-340.

Deutsche Emissionshandelsstelle im Umweltbundesamt (2010a): Leitfaden Ablauf elektronische Kommunikation. In: http://www.dehst.de/cln_153/nn_1917774/SharedDocs/Downloads/DE/VPS/VPS__Leitfaden__VPS,templateId=raw,property=publicationFile.pdf/VPS_Leitfaden_VPS.pdf, zugegriffen am 07.12.2010.

Deutsche Emissionshandelsstelle im Umweltbundesamt (2010b): Zuteilung 2008 - 2012. In: http://www.dehst.de/cln_153/nn_477208/DE/Teilnehmer/Anlagenbetreiber/Zuteilung__2008-2012/Zuteilung__2008-2012__node.html?__nnn=true&__nnn=true#doc477236bodyText1, zugegriffen am 04.08.2010.

Deutsche Post (2009): Identitätsprüfung. In: http://www.deutschepost.de/dpag?xmlFile=1015469, zugegriffen am 09.12.2009.

Deutscher Bundestag (o. J.): Basisinformationen über den Vorgang. In: http://dipbt.bundestag.de/extrakt/ba/WP16/154/15407.html, zugegriffen am 07.02.2011.

Deutschland-Online (2009): Deutschland-Online Vorhaben Kfz-Wesen - Feinkonzept zur Stufe 1. In: http://www.kdv-is.de/index.php?eID=tx_nawsecuredl&u=0&file=uploads/tx_cqeventure/KFZ_DOL.pdf&t=1296659705&hash=61c8e15ee8be8d6dca064d0bf0f77fc7, zugegriffen am 01.02.2011.

Deutschland-Online (2010): Deutschland-Online Vorhaben "Kfz-Wesen". In: http://www.kdv-is.de/index.php?eID=tx_nawsecuredl&u=0&file=uploads/tx_cqeventure/DOL-Kfz-Wesen_Konzept_09.04.2009.pdf&t=1296659705&hash=89ba8fa622c806ffbb2ddd1d0f9c94fa, zugegriffen am 01.02.2011.

Die Beauftragte der Bundesregierung für Informationstechnik (2010): IT-Investitionsprogramm. In: http://www.cio.bund.de/cae/servlet/contentblob/1124074/publicationFile/90317/it_investitionsprogramm_massnahmen_uebersicht_download.pdf, zugegriffen am 07.12.2010.

Dietrich, C. J./ Rossow, C./ Pohlmann, N. (2010): Studie - Zwischenbericht: „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test“. In: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/restrisiken.pdf?__blob=publicationFile, zugegriffen am 19.01.2012.

DIHK (2009): Elektronische Gewerbeanmeldung - Forderung zur Effizienzsteigerung und Entbürokratisierung im Bereich der Antrags- und Genehmigungsverfahren für Unternehmensgründungen. In:

http://www.dihk.de/ressourcen/downloads/position_e_gewerbemeldung.pdf, zugegriffen am 01.02.2011.

Dozier, D. M./ Ehling, W. P. (1992): Evaluation of Public Relations Programs: What the Literature Tells Us About Their Effects. In: Excellence in Public Relations and Communication Management. Ed.: Grunig, J.E., Lawrence Erlbaum Associates, Hillsdale 1992, S. 159-184.

Dunstone, T. (2000): Interview with Richard E Norton, International Biometric Industry Association (IBIA). In: http://www.austlii.org/au/journals/PLPR/2002/32.html, zugegriffen am 01.02.2011.

Eastlick, M. A./ Lotz, S. L./ Warrington, P. (2006): Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. In: Journal of Business Research, 59 (2006) 8, S. 877-886.

Euro Security (2010): Der neue PA: Segen oder Sicherheitsrisiko? In: http://www.eurosecglobal.de/deutsch/index.php?option=com_content&view=article&id=2910:der-neue-pa-segen-oder-sicherheitsrisiko-&catid=52:smartcardskartenmanager&Itemid=82, zugegriffen am 09.05.2011.

Executive Office of the President (2003): E-Authentication Guidance for Federal Agencies.

Fawer, U. (2009): Untersuchung zur Marktentwicklung von Identitätskarten in Europa mittels Szenario-Technik. iimt University Press, Fribourg 2009.

Finanzamt (2010): Ablaufbeschreibung der Registrierung im ElsterOnline-Portal. In: http://www.finanzamt.bayern.de/informationen/elster/Ablaufbeschreibung-der-Registrierung-im-ElsterOnline.pdf, zugegriffen am 15.12.2010.

Fraunhofer Fokus (2010): Kfz-Zulassung: ohne Behördengang, ohne Wartezeit. In: http://www.fokus.fraunhofer.de/de/elan/_docs/pressetext_ekfz_de_100331.pdf, zugegriffen am 01.02.2010.

Gefen, D. (2000): E-Commerce: The role of familiarity and trust. In: Omega: The International Journal of Management Science, 28 (2000) 6, S. 725-737.

Gerstbach, P. (2004): Die österreichische Bürgerkarte. In: http://www.rechtsprobleme.at/doks/burgerkarte-gerstbach.pdf, zugegriffen am 07.02.2011.

Grote, J. H./ Keizer, D./ Kenzler, D./ P., K./ Meinel, C./ Schnjakin, M./ Zoth, L. (2010): Vom Client zur App - Ideenkatalog zur Zukunft der Software der Personalausweisnutzung. In: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/ideenkatalog_software_npa.pdf?__blob=publicationFile, zugegriffen am 19.01.2012.

Grunig, J. E./ Hunt, T. (1984): Managing public relations. Holt, Rinehart and Winston New York 1984.

Hart, C./ Blackshaw, P. (2005): Communication Breakdown: Can you compete in the consumer generated media dialogue revolution? In: Marketing Management, 14 (2005) 6, S. 24.

Hensel, M./ Wirsam, J. (2008): Diffusion von Innovationen - Ein Beispiel Voice over IP. Sepktrum wirtschaftswissenschaftliche Forschung, Gabler Verlag, Wiesbaden 2008.

Herrmann, A./ Huber, F. (2009): Produktmanagement: Grundlagen, Methoden, Beispiele. Gabler Verlag, Wiesbaden 2009.

Hinz, R. (2006): Die virtuelle Poststelle der DEHSt. In: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/VirtuellePoststelle/AntragZuteilgEmissionsberechtHinz_pdf.pdf?__blob=publicationFile, zugegriffen am 07.12.2010.

Homburg, C./ Krohmer, H. (2009): Marketingmanagement: Strategie-, Instrumente-, Umsetzung- und Unternehmensführung. Gabler Verlag, Wiesbaden 2009.

Home Office (2010a): Identity Cards. In: http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/passports-andimmigration/id-cards/, zugegriffen am 15.12.2010.

Home Office (2010b): Identity Cards and National Identity Register to be scrapped. In: http://www.homeoffice.gov.uk/media-centre/press-releases/identity-cards-scrapped1, zugegriffen am 26.01.2011.

Home Office (2010c): Why we need ID Cards. In: www.homeoffice.gov.uk/passports-and-immigration/id-cards/why-we-need-id-cards/, zugegriffen am 15.12.2010.

Home Office (2011): Cancellation of identity cards. In: http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1690.htm, zugegriffen am 26.01.2011.

Information & Communications Technology branch Multi-factor Authentication Solution Selection Issues. In: http://www.e.govt.nz/standards/e-gif/authentication/guide-multi-factor-auth/chapter6.html, zugegriffen am 18.12.2009.

Jarvenpaa, S. L./ Tractinsky, N./ Vitale, M. (2000): Consumer trust in an Internet store. In: Information Technology Management, 1 (2000) 1, S. 45-71.

Jones, S./ Wilikens, M./ Morris, P./ Masera, M. (2000): Trust requirements in e-business. In: Communications of the ACM, 43 (2000) 12, S. 81-87.

Kim, D. J./ Ferrin, D. L./ Rao, H. R. (2008): A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. In: Decision Support Systems, 44 (2008) 2, S. 544-564.

Kimpeler, S./ Georgieff, P./ Beckert, B./ Postler, J. (2005): IT-Einsatz und Umsetzung von E-Government in den Kommunalverwaltungen Baden-Württembergs Karlsruhe2005.

Klump, D. (2006): Der Beitrag von E-Government zur Modernisierung der Gesellschaft. In: http://www.execupery.com/dokumente/ITs_TIME__Klumpp_Beitrag.pdf, zugegriffen am 01.02.2011.

Kollmann, T. (1998): Akzeptanz innovativer Nutzungsgüter und -systeme. Gabler Verlag, Wiesbaden 1998.

Kommune21 (2010): Priorität fürs Kfz-Wesen. In: http://www.kommune21.de/meldung_10984, zugegriffen am 01.02.2011.

König, K. (1995): Neue Verwaltung oder Verwaltungsmodernisierung. Verwaltungspolitik in den 90er Jahren. In: Die öffentliche Verwaltung, 48 (1995) 9, S. 349-358.

Kraftfahrt-Bundesamt (2009): Neuzulassungen - Jahresbilanz der Neuzulassungen 2009. In: http://www.kba.de/cln_007/nn_125264/DE/Statistik/Fahrzeuge/Neuzulassungen/neuzulassungen__node.html?__nnn=true#rechts, zugegriffen am 29.11.2010.

Krcmar, H. (2009): Gesamtwirtschaftliches Potenzial und (wirtschafts-) politische Aktualität. In: Elektronischer Personalausweis - Wirtschaftliche Bedeutung und Anwendungstests. Eds.: Thielmann, H.; Ziemer, A., München 2009, S. 12-28.

Krcmar, H. (2010): Informationsmanagement. 5., vollständig überarbeitete und erweiterte Auflage, Springer Verlag, Berlin 2010.

Lanier, C. D./ Saini, A. (2008): Understanding consumer privacy: A review and future directions. In: Academy of Marketing Science Review, 12 (2008) 2, S. 1-45.

Lee, M. K. O./ Turban, E. (2001): A trust model for consumer internet shopping. In: International Journal of electronic commerce, 6 (2001) 1, S. 75-92.

Löhe, M./ Tschichholz, M. (2010): ARGE eKfz. In: http://www.fokus.fraunhofer.de/de/elan/projekte/national/laufende_projekte/arge_ekfz/index.html, zugegriffen am 29.11.2010.

Markus, M. L./ Keil, M. (1994): If we build it, they will come: Designing information systems that people want to use. In: Sloan Management Review, 35 (1994), S. 11-11.

Matsumoto, T./ Matsumoto, H./ Yamada, K./ Hoshino, S. (2002): Impact of Artifical "Gummy" Fingers on Fingerprint Systems. In: Proceedings of the Optical Security and Counterfeit Deterrence Techniques IV. 2002, S. 275-289.

Mayer, H.-P. (2010): Bürger-Service-Portal. In: http://files.messe.de/cmsdb/D/007/22143.pdf, zugegriffen am 07.12.2010.

Mayring, P. (2010): Qualitative Inhaltsanalyse - Grundlagen und Techniken 11., aktualisierte und überarbeitete Auflage, Beltz Verlag, Weinheim, Basel 2010.

McKnight, D. H./ Chervany, N. L. (2002): What trust means in E-Commerce customer relationships: an interdisciplinary conceptual typology. In: International Journal of Electronic Commerce, 6 (2002) 2, S. 35-59.

Mertens, P. (2009): Schwierigkeiten mit IT-Projekten der öffentlichen Verwaltung. In: Informatik-Spektrum, 32 (2009) 1, S. 42-49.

Milne, G. R./ Boza, M. E. (1998): Trust and concern in consumers' perceptions of marketing information management practices. In: Journale of Interactive Marketing, 13 (1998) 1, S. 5-24.

Mintzberg, H. (1996): Managing Government, Governing Management. In: http://gspa.grade.nida.ac.th/pdf/Dr_Nutta/PA600PP601/No3/PA600_3-2_Nutta.pdf, zugegriffen am 26.01.2011.

Morgan, R. M./ Hunt, S. D. (1994): The commitment-trust theory of relationship marketing. In: The journal of marketing, 58 (1994) 3, S. 20-38.

München.de (2010): Gewerbebehörde der Stadt München - Informationen zum An-, Ab- und Ummelden eines Gewerbebetriebs. In: http://www.muenchen.de/Rathaus/kvr/gewerbugast/gewmeld/60426/gewerbemeldungen.html, zugegriffen am 07.12.2010.

Nasir, R. M./ Ponnusamy, V./ Wazeer, M. W. (2007): An Exploratory Study on the Level of Trust towards Online Retailers among Consumers in the United Kingdom and Malaysia.

Nissenbaum, H. (2001): Securing trust online: Wisdom or Oxymoron. In: Boston University Law Review, 81 (2001) 3, S. 101-131.

o. V. (2008): Das Ende der Anonymität. In: http://www.zeit.de/online/2008/42/elektronischer-personalausweis, zugegriffen am 07.12.2009.

o. V. (2009a): Im Härtetest. In: www.vitako.de, zugegriffen am 07.02.2011.

o. V. (2009b): Neuer Personalausweis-Anwendungstest 2009-2010. In: https://bremen.de/fastmedia/36/AT_Broschuere.pdf, zugegriffen am 01.02.2011.

o. V. (2010a): (N)Onliner Atlas 2010: eGovernment - Monitor 2010. TNS Infratest GmbH, München2010a.

o. V. (2010b): (N)Onliner Atlas 2010: Eine Topographie des digitalen Grabens durch Deutschland. In: http://www.initiatived21.de/wp-content/uploads/2010/06/NONLINER2010.pdf, zugegriffen am 01.02.2011.

o. V. (2010c): Offen für die Zukunft - Kompetenz, Sicherheit und neue Geschäftsfelder. In: http://www.tns-infratest.com/presse/pdf/Presse/Offen_fuer_die_Zukunft_Offen_in_die_Zukunft.pdf, zugegriffen am 01.02.2011.

o. V. (2011a): De-Safe – Online-Safe für De-mail-Dokumente. In: http://www.de-safe.com/, zugegriffen am 16.05.2011.

o. V. (2011b): eGovernment Monitor 2011 - Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich. TNS Infratest GmbH, München2011b.

Olivero, N./ Lunt, P. (2004): Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. In: Journal of Economic Psychology, 25 (2004) 2, S. 243-262.

Open Limit (2009): Federal Government Contracts Out Bürger-Client Development for the Electronic Identity Card. In: http://www.openlimit.com/assets/files/presse/en/Federal-government-contracts-out-buerger-client.pdf, zugegriffen am 09.05.2011.

Peinel, G. E. (2008): Planung und Umsetzung von Geschäftsmodellen für eGovernmentdienste in Public Private Partnerships, Fraunhofer Series in Information and Communication Technology, Shaker Verlag, Aachen 2008.

Penski, U. (1999): Staatlichkeit öffentlicher Verwaltungen und ihre marktmäßige Modernisierung. In: Die öffentliche Verwaltung, 52 (1999) 3, S. 85-96.

Petkovic, M./ Jonker, W. (Eds.) (1998): Privacy and Security Issues in a Digital World. Data-Centric Systems and Applications, Springer Verlag, Berlin, Heidelberg 1998.

Phelps, J./ Nowak, G./ Ferrell, E. (2000): Privacy concerns and consumer willingness to provide personal information. In: Journal of Public Policy & Marketing, 19 (2000) 1, S. 27-41.

Price, G. (2008): The benefits and drawbacks of using electronic identities. In: Information Security Technical Report, 13 (2008) 2, S. 95-103.

Reichard, C. (2003): Die Ökonomiseirung des öffentlichen Sektors: Instrumente und Trends: "New Public Management" als Auslöser zunehmender Ökonomisierung der Verwaltung. Nomos 2003.

Reisen, A. (2009): Der elektronische Personalausweis und die elektronische Signatur. In: http://www.maremba.de/multimedia/01_mandantenspezifisch/maremba/PDF/Workshop_Elektronische_Signatur/2009_10_02_Workshop_Elektronische_Signatur_Stuttgart_Reisen.pdf, zugegriffen am 01.02.2011.

Rogers, E. M. (2005): Diffusion of Innovations. 5. Auflage, Free Press, New York, London, Toronto, Sydney, Singapore 2005.

Roßnagel, A./ Yildirim, N. (2002): Datenschutzgerechtes Electronic Government. In: http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2007112019649/1/DASimEG2002.pdf, zugegriffen am 26.01.2011.

Roßnagel, H. (2006): On Diffusion and Confusion – Why Electronic Signatures Have Failed. In: Proceedings of the Trust and Privacy in Digital Business. Eds.: Fischer-Hübner, S.; Furnell, S.; Lambrinoudakis, C., Springer Verlag, Kraków 2006, S. 71-80.

Rüegg-Stürm, J. (2003): Das neue St. Galler Management-Modell. In: Einführung in die Managementlehre - Band 1. Eds.: Dubs, R.; Euler, D.; Rüegg-Stürm, J.; Wyss, C.E., Haupt, Bern 2003.

Schallbruch, M. (2010): Elektronische Identitäten im Internet und die Einführung des elektronischen Personalausweises. In: Netzwelt - Wege, Werte, Wandel. Eds.: Klumpp, D.; Kubicek, H.; Roßnagel, A.; Schulz, W., Springer Verlag, Heidelberg, Dordrecht, London, New York 2010, S. 211-220.

Scheer, A.-W. (1997): Wirtschaftsinformatik : Referenzmodelle für industrielle Geschäftsprozesse. 7. ed., Springer, Berlin [u.a.] 1997.

Scheer, A./ Kruppke, H./ Heib, R. (2003): E-Government. Springer Verlag, Berlin, Heidelberg, New York 2003.

Scheffel, U. (2010): Technische Voraussetzungen: Kartenleser, teilweise subventioniert. In: http://www.tomshardware.de/Personalausweis-rfid,testberichte-240664-6.html, zugegriffen am 09.05.2011.

Schewe, G./ Nienaber, A.-M. (2009): Vertrauenskommunikation und Innovationsbarrieren: Theoretische Grundlagen. In: Kommunikation als Erfolgsfaktor im Innovationsmanagement: Strategien im Zeitalter der Open Innovation Eds.: Zerfaß, A.; Möslein, K.M., Gabler Verlag, Wiesbaden 2009, S. 227-242.

Schmeh, K. (2009): Elektronische Ausweisdokumente. Hanser Fachbuchverlag, Freiburg 2009.

Schoeman, F. (Ed.) (1984): Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, Cambridge 1984.

Schoenbachler, D. D./ Gordon, G. L. (2002): Trust and customer willingness to provide information in database-driven relationship marketing. In: Journal of Interactive Marketing, 16 (2002) 3, S. 2-16.

Scholz, S. (2004): Internet-Politik in Deutschland - Vom Mythos der Unregulierbarkeit, Universität Bonn, Universität Bonn, Bonn 2004.

Shankar, V./ Urban, G. L./ Sultan, F. (2002): Online trust: a Stakeholder perspective, concepts, implications, and future directions. In: The Journal of Strategic Information Systems, 11 (2002) 3-4, S. 325-344.

Shneiderman, B. (2000): Designing trust into Online Experiences. In: Communications of the ACM, 43 (2000) 12, S. 57-59.

Statistisches Bundesamt Deutschland (2009a): Gewerbe- und Insolvenzmeldungen. In: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/UnternehmenGewerbeInsolvenzen/Gewerbeanzeigen/Tabellen/Content50/Gewerbeabmeldungen__WZ,templateId=renderPrint.psml, zugegriffen am 01.02.2011.

Statistisches Bundesamt Deutschland (2009b): Gewerbeanmeldungen. In: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/UnternehmenGewerbeInsolvenzen/Gewerbeanzeigen/Tabellen/Content50/Gewerbeanmeldungen__WZ,templateId=renderPrint.psml, zugegriffen am 01.02.2011.

Stevens, T./ Elliott, J./ Hoikkanen, A./ Maghiros, I./ Lusoli, W. (2010): The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies. In: JRC Scientific and Technical Reports (2010).

Sullivan, C. (2010): Digital Identity. University of Adelaide Press 2010.

Tönjes Holding AG (2010a): Fortschritt und Innovation. In: http://www.toenjes-portal.de/dokumente/Fortschritt%20und%20Innovation_a.pdf, zugegriffen am 01.02.2010.

Tönjes Holding AG (2010b): Unser Kennzeichen ist Erfahrung - Häufige Fragen/FAQ. In: http://www.toenjes-portal.de/index.php/zulassungsdienst.html, zugegriffen am 29.11.2010.

Tönjes Holding AG (2010c): Unser Kennzeichen ist Erfahrung - Zulassungsdienst. In: http://www.toenjes-portal.de/index.php/zulassungsdienst.html, zugegriffen am 29.11.2010.

Turner, T./ Schwager, A./ Guo, Z. (2005): Verifying e-Government Market Segments. In: Proceedings of the Proceedings of the International Conference on e-Government (ICEG 2005). Ed.: Remenyi, D., Academic Conferences Limited, Ottawa 2005, S. 441-451.

UK Cabinet Office (2002): Registration and Authentication: e-Government Strategy Framework Policy and Guidelines (Report)2002.

Umweltbundesamt (2010a): Allgemeine Informationen über den Emissionshandel. In: http://www.dehst.de/cln_153/nn_1945078/DE/Emissionshandel/emissionshandelNode.html?__nnn=true, zugegriffen am 07.12.2010.

Umweltbundesamt (2010b): Identifiation - Informationen zur elektronischen Kommunikation. In: http://www.dehst.de/nn_476144/DE/Service/elektronische__Kommunikation/Elektronische__Kommunikation__Identifikation/Elektronische__Kommunikation__Identifikation__node.html?__nnn=true, zugegriffen am 07.12.2010.

Umweltbundesamt (2010c): Informationen zur Emissionsberichterstattung 2010. In: http://www.dehst.de/cln_153/nn_476204/DE/Teilnehmer/Anlagenbetreiber/Berichterstattung__2010/Emissionsberichterstattung__2010__node.html?__nnn=true, zugegriffen am 07.12.2010.

Umweltbundesamt (2010d): Installationshandbuch: Das elektronische Postfach (EP). In: http://www.dehst.de/cln_162/nn_476194/SharedDocs/Downloads/DE/VPS/VPS__Installationsanleitung,templateId=raw,property=publicationFile.pdf/VPS_Installationsanleitung.pdf, zugegriffen am 01.02.2011.

Urban, G. L./ Amyx, C./ Lorenzon, A. (2009): Online trust: State of the art, new frontiers, and research potential. In: Journal of Interactive Marketing, 23 (2009) 2, S. 179-190.

Urban, G. L./ Sultan, F./ Qualls, W. J. (2000): Placing Trust at the Center of your Internet Strategy. In: Sloan Management Review, 42 (2000) 1, S. 39-48.

Valkenburg, P./ Meijers, W./ Lycklama, D./ Jansen, V. (2010): E-identity as a business. In: http://www.everett.nl/content/index.php?option=com_docman&task=doc_download&gid=42, zugegriffen am 26.01.2011.

Venkatesh, V./ Morris, M. G./ Davis, G. B./ Davis, F. D. (2003): User Acceptance of Information Technology: Toward a Unified View. In: MIS Quarterly, 27 (2003) 3, S. 425-478.

Verbraucherzentrale Berlin (2010): Der neue elektronische Personalausweis - Die wichtigsten Fragen und Antworten. In: http://www.vz-berlin.de/UNIQ130555110616928/link804101A.html, zugegriffen am 16.05.2011.

Vogt, S. (2010): Neuer elektronischer Personalausweis kommt im November: Ein Aufwand wie bei der Euro-Einführung. In: http://www.derwesten.de/staedte/bochum/Ein-Aufwand-wie-bei-der-Euro-Einfuehrung-id3844712.html, zugegriffen am 07.02.2011.

Walczuch, R./ Lundgren, H. (2004): Psychological antecedents of institution-based Consumer trust in e-Retailing. In: Information & Management, 42 (2004) 1, S. 159-177.

Wang, S./ Beatty, S. E./ Foxx, W. (2004): Signaling the trustworthiness of small online retailers. In: Journal of Interactive Marketing, 18 (2004) 1, S. 53-69.

Weiber, R. (1992): Diffusion von Telekommunikation: Problem der kritischen Masse. Gabler Verlag, Wiesbaden 1992.

Yildirim, N. (2004): Datenschutz im Electronic Government: Risiken, Anforderungen und Gestaltungsmäglichkeiten für ein datenschutzgerechtes und rechtsverbindliches eGovernment. Deutscher Universitäts-Verlag 2004.

Zerdick, A./ Picot, A./ Schrape, K./ Artopé, A./ Goldhammer, K./ Heger, D. K./ Lange, U. T./ Vierkant, E./ Lopez-Escobar, E./ Silverstone, R. (2001): Die Internet-Ökonomie: Strategien für die digitale Wirtschaft. Springer, Berlin, Heidelberg 2001.

Zerfaß, A. (2009): Kommunikation als konstitutives Element im Innovationsmanagement. In: Kommunikation als Erfolgsfaktor im Innovationsmanagement: Strategien im Zeitalter der Open Innovation Eds.: Zerfaß, A.; Möslein, K.M., Gabler Verlag, Wiesbaden 2009, S. 23-56.